МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

«ДОПУЩЕНИЙ ДО ЗАХИСТУ»
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«17» 06 2026 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «бакалавр»

РОЗРОБКА ІНФОРМАЦІЙНОЇ МОДЕЛІ ОЦІНЮВАННЯ КРИТИЧНОСТІ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 125 «Кібербезпека та захист інформації»

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»

Виконав: студент 4381 групи
Коломієць І.Л. _____
(прізвище та ініціали) (підпис_

Керівник роботи: доцент кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
(посада, науковий ступінь, вчене звання)
Турти М.В _____
(прізвище та ініціали) (підпис_

Миколаїв – 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

Спеціальність **125«Кібербезпека та захист інформації»**
Освітня програма **«Системи технічного захисту інформації, автоматизація її обробки»**

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ
_____ С.М. Нужний
«10» 02 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття ступеня вищої освіти «бакалавр»

Студенту **Коломійцю Івану Леонідовичу**
(Прізвище, ім'я, по батькові)

1. Тема роботи: Розробка інформаційної моделі оцінювання критичності інформації та інформаційних систем

Керівник роботи доцент кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент Турти Марина Валентинівна

Затверджені наказом ректора №286-уч від 22.04.2026 р.

2. Термін подання роботи: 10.06.2026 р.

3. Вихідні дані по роботі: теоретичні основи побудови захищених комп'ютерних систем, ISO/IEC 27005, NIST SP 800-60, FIPS 199, IACS UR E22, НД ТЗІ 3.6-005-21.

4. Перелік питань, що належать до розробки: провести аналіз чинних міжнародних та національних стандартів (зокрема ISO/IEC 27005, NIST SP 800-60, IACS UR E22, НД ТЗІ 3.6-005-21) у сфері категоріювання активів та виявити недоліки існуючих підходів до оцінки критичності інформаційних систем; розробити інформаційну модель оцінювання критичності, яка формалізує залежності між впливовими факторами, і базові алгоритми для автоматизованого розрахунку інтегрального індексу критичності; провести апробацію розроблених алгоритмів для підтвердження адекватності та працездатності моделі.

5. Перелік презентаційних матеріалів: Актуальність, мета і завдання роботи. Нормативно-правова база розробки. Оцінка критичності ОКІІ. Методика IACS UR E22. Методика НД ТЗІ 3.6-005-21. Базові алгоритми. Інформаційна модель. Результати апробації моделі. Висновки.

6. Консультант-внутрішній рецензент роботи (нормоконтроль)

Прізвище, ініціали та посада	Дата подання роботи на рецензування	Дата отримання рецензії	Підпис
Передерій В.І, професор кафедри КТІБ	2.06.26	5.06.26	

7. Дата видачі завдання 10.02.2026 р.

КАЛЕНДАРНИЙ ПЛАН

Номер	Назва етапів роботи	Терміни виконання	Примітка
1	Вибір теми, визначення мети, завдань, об'єкта та предмета дослідження	10.02.2026	
2	Попередній варіант оглядових розділів, підбір і опрацювання списку використаних джерел	20.03.2026	
3	Попередній варіант повної КР	15.04.2026	
4	Складання ЄДКІ зі спеціальності на ступінь «бакалавра»	16.04.2026 14.05.2026	
5	Попередній варіант презентації	29.05.2026	
6	Подання на кафедру КТІБ тексту остаточного варіанту роботи, підписаного її керівником в електронному форматі (*.pdf) разом із заявами щодо самостійності виконання роботи та ідентичності друкованої та електронної версій роботи (Додатки 1 і 2 «Порядку здійснення заходів з перевірки робіт на наявність текстових збігів/ідентичності/схожості із використанням програмно-технічних засобів», який введений в дію наказом ректора НУК за №20 від 20.01.2020 р.) Отримання внутрішньої рецензії	05.06.2026	не пізніше, ніж за 14 діб до захисту (згідно п.4.1 зазначеного Порядку)
7	Отримання висновку керівника Отримання висновку кафедри щодо наявності/відсутності плагіату в роботі Попередній захист роботи на засіданні кафедри КТІБ Висновок кафедри про КР, допуск до захисту	10.06.2026	
8	Отримання зовнішньої рецензії	15.06.2026	
9	Підготовка презентації та доповіді	17.06.2026	
10	Подання на кафедру КТІБ: — друкованого і зшитого варіанту пояснювальної записки до кваліфікаційної роботи та/або (за рішенням кафедри) електронного варіанту в форматі *.pdf — друкованого варіанту презентації (в 5-ти екземплярах в разі захисту оф-лайн, в одному екземплярі в разі захисту он-лайн (за рішенням кафедри)) та електронного варіанту презентації; — зовнішньої рецензії; — документів щодо відсутності плагіату і передачі авторських прав; — файлу-опису кваліфікаційної роботи (згідно Додатку до наказу ректора НУК за №287-уч від 19.05.2020 р.).	22.06.2026	
11	Захист кваліфікаційної роботи	24-25.06.2026	

Студент _____ (підпис) Коломієць І.Л. (ПІБ)

Керівник роботи _____ (підпис) Турти М.В. (ПІБ)

АНОТАЦІЯ

Коломієць І.Л. **Розробка інформаційної моделі оцінювання критичності інформації та інформаційних систем**

Кваліфікаційна робота на правах рукопису на здобуття ступеня вищої освіти «бакалавр» за освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 «Кібербезпека та захист інформації» Національного університету кораблебудування імені адмірала Макарова, Миколаїв, 2026.

Кваліфікаційна робота присвячена актуальній темі – підвищенню ефективності систем управління інформаційною безпекою. Об'єктом дослідження в даній роботі є процеси категоріювання інформації та інформаційних систем. Предметом дослідження в даній роботі є метрики та алгоритми оцінювання критичності інформації та інформаційних систем. Метою роботи є підвищення ефективності процесу категоріювання інформаційних ресурсів шляхом розробки математично обґрунтованої інформаційної моделі та автоматизованих алгоритмів оцінювання критичності інформації й інформаційних систем. Методами дослідження є методи управління інформаційною безпекою, методи системного аналізу та теорії прийняття рішень, методи алгоритмізації.

У роботі проведено аналіз чинних міжнародних та національних стандартів у сфері категоріювання активів та виявлені недоліки існуючих підходів до оцінки критичності інформаційних систем; розроблено інформаційну модель оцінювання критичності, яка формалізує залежності між впливовими факторами, і базові алгоритми для автоматизованого розрахунку інтегрального індексу критичності; здійснено апробацію розроблених алгоритмів і підтверджено адекватність та працездатність моделі.

Робота має практичну значимість, її результати можуть бути використані при проєктуванні систем безпеки інформації та в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації».

Ключові слова: кібербезпека, категоріювання інформації, категоріювання інформаційних систем, інформаційна модель, інтегральний індекс критичності.

ABSTRACT

Kolomiets I.L. **Development of an information model for assessing the criticality of information and information systems**

Qualification work in the form of a manuscript on receiving a higher education degree "Bachelor" in the educational and professional program «Systems technical protection of information, automation of its processing» specialty 125 «Cybersecurity and Information Protection» – Admiral Makarov National University of Shipbuilding, Mykolaiv, 2026.

The qualification work is devoted to a topical issue - increasing the efficiency of information security management systems. The object of research in this work is the processes of categorization of information and information systems. The subject of research in this work is metrics and algorithms for assessing the criticality of information and information systems. The purpose of the work is to increase the efficiency of the process of categorization of information resources by developing a mathematically based information model and automated algorithms for assessing the criticality of information and information systems. The research methods are information security management methods, systems analysis methods and decision-making theories, and algorithmization methods.

In thesis current international and national standards in the field of asset categorization have been analyzed and shortcomings of existing approaches to assessing the criticality of information systems have been identified; information model for assessing criticality, which formalizes the dependencies between influential factors, and basic algorithms for automated calculation of the integral criticality index have been developed; the developed algorithms have been tested and the adequacy and operability of the model have been confirmed.

The work has practical significance, its results can be used in the design of information security systems and in the educational process in the specialty F5 "Cybersecurity and Information Protection".

Keywords: cybersecurity, information categorization, information systems categorization, information model, integral criticality index.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

FIPS – Federal Information and Information Systems;

GRC – Governance, Risk, and Compliance;

IIoT – Industrial Internet of Things;

IRM – Integrated Risk Management;

NIST – National Institute of Standards and Technology;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційна система;

ІТ – інформаційні технології;

КІ – критична інфраструктура;

ОІД - об’єкт інформаційної діяльності;

ОКІ - об’єкт критичної інфраструктури;

ОКІІ - об’єкт критичної інформаційної інфраструктури;

СБІ – система безпеки інформації.

ВСТУП

Сучасна повномасштабна війна супроводжується повноцінною кібервійною. В цих умовах питання захисту інформаційних ресурсів, особливо ресурсів і інформаційно-комунікаційних систем (ІКС) об’єктів критичної інфраструктури (ОКІ), набуло стратегічного значення. Оскільки жодна організація не має безмежних фінансових чи людських ресурсів, то обробка ризиків, асоційованих з певними інформаційними активами і ІКС, здійснюється за їх пріоритетами, що вимагає чіткої процедури їх категорзації.

Необхідність забезпечення швидкої і безпомилкової категоризації і, відповідно, актуальність даної роботи зумовлені кількома ключовими факторами:

– наявність законодавчих вимог щодо категоризації об’єктів критичної інформаційної інфраструктури (ОКІІ) [4, 17, 18, 34, 35, 37, 38], інформації та інформаційних систем [23, 31, 36];

– наявність спеціалізованих міжнародних галузевих стандартів, таких як IACS UR E22 [9], що висувають вимоги до комп'ютеризованих систем, відповідно до специфіки конкретних інфраструктурних секторів;

– необхідність багатократного повторення процедури категоризації в умовах динамічної зміни ландшафту інформаційних технологій (ІТ) з метою адаптації систем безпеки інформації до змінних умов функціонування.

На сьогодні у сфері оцінювання ризиків та критичності активів сформовано потужну науково-методологічну базу, яка включає зарубіжні стандарти та фреймворки (такі як ISO/IEC 27005 [11] та ISO/IEC 27001 [10], FIPS 199 [8], NIST SP 800-30 [12], NIST SP 800-60 [13], NIS 2 [4] тощо), зарубіжні [3, 12, 13] і вітчизняні наукові здобутки (роботи В. О. Хорошко [33], О. Г. Корченко [24], О. Задерейко [21], М. В. Турти [47, 48], та ін. [21, 22, 27, 28, 32, 45, 46, 49]). Попри значні теоретичні напрацювання, на практиці залишаються відкритими такі проблеми як суб'єктивізм та невизначеність

експертних оцінок, складність врахування взаємозв'язків (каскадного ефекту) різних об’єктів категоризації в умовах змінного ІТ-ландшафту.

Наявні на ринку програмні продукти, які теоретично можуть бути використані для оцінювання критичності систем «на льоту» ([1, 2, 5, 16]) надзвичайно дорогі, складні в інтеграції і не відповідають вимогам вітчизняної нормативно-правової бази.

Метою даної роботи є підвищення ефективності процесу категоріювання інформаційних ресурсів шляхом розробки математично обґрунтованої інформаційної моделі та автоматизованих алгоритмів оцінювання критичності інформації й інформаційних систем.

Для досягнення поставленої мети необхідно вирішити наступні **задачі**:

– провести аналіз чинних міжнародних та національних стандартів (зокрема ISO/IEC 27005, NIST SP 800-60, НД ТЗІ 3.6-005-21, IACS UR E22) у сфері категоріювання активів та виявити недоліки існуючих підходів до оцінки критичності інформаційних систем;

– розробити інформаційну модель оцінювання критичності, яка формалізує залежності між впливовими факторами, і базові алгоритми для автоматизованого розрахунку інтегрального індексу критичності;

– провести апробацію розроблених алгоритмів для підтвердження адекватності та працездатності моделі.

Об’єктом дослідження в даній роботі є процеси категоріювання інформації та інформаційних систем (ІС).

Предметом дослідження в даній роботі є метрики та алгоритми оцінювання критичності інформації та інформаційних систем.

Методами дослідження є методи управління інформаційною безпекою, методи системного аналізу та теорії прийняття рішень, методи алгоритмізації.

Робота має практичну значимість, її результати можуть бути використані при проєктуванні систем безпеки інформації (СБІ) та в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації».

РОЗДІЛ 1. АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОЦІНЮВАННЯ КРИТИЧНОСТІ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Аналіз понятійного апарату і ризик-орієнтованого підходу до оцінювання критичності інформації та інформаційних систем

Ефективна розробка та впровадження автоматизованих систем оцінювання захищеності сучасних об'єктів автоматизації вимагає чіткої формалізації базових понять кібербезпеки. Центральне місце у цьому процесі посідає категорія «інформаційного активу». Відповідно до визначення, наведеного в поточній редакції Закону України «Про інформацію», інформація розглядається як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [41].

У контексті комп'ютеризованих та розподілених середовищ цей термін трансформується в поняття інформаційного активу, що охоплює не лише самі дані, а й інфраструктуру їх обробки, тобто інформаційний актив - це дані чи знання на будь-яких носіях (тобто матеріальний чи нематеріальний об’єкт), або інформаційні системи, які забезпечують безперебійну роботу організації і, відповідно, мають цінність для неї та вимагають захисту. Міжнароднийстандарт ISO/IEC 27001:2022 [10], якому відповідає ДСТУ ISO/IEC 27001:2023 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги» (ISO/IEC 27001:2022, IDT) [19], розглядає як об’єкт захисту саме інформаційний актив.

Серед інформаційних активів можна виділити [45]:

а) активи інформації різного змісту та призначення: файли даних, бази даних та знань, контракти та угоди, дослідницька інформація, настанови для користувачів, журнали аудиту та архівна інформація, системна документація, плани і заходи підтримки безперервності бізнесу тощо;

б) активи програмного забезпечення (ПЗ): прикладне ПЗ, системне ПЗ, утиліти, засоби розробки ПЗ;

в) активи обладнання: обчислювальна техніка, мережеве та інше телекомунікаційне обладнання, змінні носії інформації, смартфони тощо;

г) активи послуг: обчислювальні послуги, телекомунікаційні послуги, комунальні послуги тощо;

д) активи персоналу: кадри, їх кваліфікація, навички та досвід;

е) нематеріальні активи: репутація організації та її імідж.

Згідно з методологією міжнародного стандарту ISO/IEC 27005:2022 [11], якому відповідає ДСТУ ISO/IEC 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки» (ISO/IEC 27005:2022, IDT) [20], першим етапам управління ризиками є ідентифікація активів, оскільки саме вони є носіями цінності для організації та об'єктами потенційного впливу загроз [19]. При цьому в комп'ютерних системах активи поділяються на первинні (безпосередньо інформація або бізнес-процеси) та допоміжні (апаратні засоби, програмне забезпечення, мережеві компоненти, персонал).

Специфіка сучасного стану розвитку IT-інфраструктур полягає у розмиванні традиційного безпекового периметру підприємств. Широке використання хмарних сховищ, концепцій використання власних пристроїв працівників (BYOD) та неконтрольоване застосування сторонніх сервісів («Shadow IT») призводять до значного ускладнення структури активів, що підтверджується сучасними практичними дослідженнями аналітиків [6, 7, 27].

Другим базовим поняттям досліджуваної предметної області є «критичність» інформації та інформаційних систем (ІС). Аналіз нормативного документа НД ТЗІ 3.6-005-21 свідчить, що критичність системи та інформації безпосередньо корелює з визначенням «порядку категоріювання безпеки інформаційної системи» [31]. Категорування безпеки, у свою чергу, виступає інструментом диференціації вимог до захисту залежно від ступеня наслідків, до

яких може призвести порушення властивостей безпеки. Розрахунок критичності традиційно спирається на базову тріаду інформаційної безпеки КСД або англійською - CIA:

К – конфіденційність (англ. confidentiality - C) – властивість інформації бути недоступною або закритою для неавторизованих осіб, сутностей чи процесів;

Ц - цілісність (англ. integrity - I)– властивість інформації бути захищеною від несанкціонованої модифікації або знищення;

Д – доступність (англ. availability - A)- властивість інформації бути доступною і готовою до використання за запитом від уповноваженої на почочний час авторизованої особи, сутності чи процесу.

Міжнародна практика, представлена американським стандартом FIPS Publication 199, визначає, що категорування безпеки має встановлювати потенційний негативний вплив («potential impact») на діяльність організації, її активи чи окремих осіб у разі настання інциденту [8]. Формалізація рівнів цього впливу здійснюється через градацію збитків: від низького (низький рівень шкідливих наслідків) до високого (катастрофічні наслідки для функціонування установ або національної безпеки) [8, 24, 27, 32, 33, 46, 49].

Аналогічний підхід закладено вітчизняних методиках оцінювання критичності ОКІ та ОКІІ, де критичність активу інтерпретується як міра негативних наслідків порушення функціонування конкретної ІС чи збереження певного масиву даних для виконання ОКІ їх основних функцій [17, 38].

У багатьох секторах критичної інфраструктури (КІ), в тому числі у секторі «Транспорт», підсектором котрого є «Морський та внутрішній водний транспорт» інформаційне моделювання процесів класифікації активів повинно обов'язково враховувати каскадний ефект [3, 12, 13, 21, 24, 27, 32, 33, 46, 49], коли відмова елемента ІС викликає ланцюгову реакцію, наприклад, відмова елемента автоматизованої системи керування може викликати зупинку технологічних процесів.

Третьою складовою понятійного апарату є «ризик-орієнтований підхід», який у сучасній практиці кібербезпеки трансформувався з рекомендаційного методу у загальнообов'язкову законодавчу вимогу. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», правове регулювання та технічний захист мають будуватися на основі аналізу ризиків та категоризації об’єктів інформаційної інфраструктури [43]. Сутність ризик-орієнтованого підходу полягає у відмові від концепції «абсолютної безпеки» на користь досягнення «прийнятного рівня ризику». Це означає, що інтенсивність та вартість заходів захисту повинні бути прямо пропорційними критичності активу та рівню загроз, що діють на нього.

Зарубіжний досвід реалізації цього підходу відображений у Директиві NIS 2 (Directive EU 2022/2555), яка встановлює вимогу щодо гармонізації заходів кібербезпеки з реальними ризиками, зазначаючи, що організації повинні впроваджувати «заходи з управління ризиками безпеки, які є доречними та пропорційними для запобігання або мінімізації впливу інцидентів» [4]. На рівні технічних інструкцій США цей підхід деталізується у фреймворку NIST SP 800-30, де ризик визначається як функція ймовірності реалізації загрози та ступеня негативного впливу (критичності) на цільову систему [14].

Проте аналіз практичних звітів CERT-UA та інцидентів у критичній інфраструктурі України підтверджує, що статичний ризик-орієнтований підхід часто не встигає за динамікою загроз [23, 25, 31]. Традиційні експертні методи оцінювання ризиків, що виконуються дискретно (наприклад, один раз на рік), швидко втрачають актуальність.

У листопаді 2025 року Кабінет Міністрів України постановою №1470 [34] затвердив зміни до постанови №518 2019 року, виклавши Загальні вимоги до кіберзахисту ОКІ в новій редакції. «Замість статичного виконання вимог, нова модель спонукає операторів до безперервного циклу управління ризиками, що дозволяє концентрувати ресурси на найбільш критичних напрямах» [46]. На виконання постанови №1470 Адміністрація Держспецзв’язку Наказом від

30.01.2026 № 75 [36] скасувала чинність наказів від 30.01.2025 №54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту» і від 06 жовтня 2021 року № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами) та затвердила Каталог заходів з кіберзахисту, Базові заходи з кіберзахисту, Форму плану кіберзахисту та Методичні рекомендації щодо здійснення заходів з кіберзахисту.

Науковці також наголошують на необхідності переходу до кількісного оцінювання критичності інформаційних ресурсів в ІС з метою оперативного перерозподілу захисних ресурсів в умовах постійних кібератак [46, 47].

Таким чином, інформаційні активи, критичність та ризик-орієнтований підхід утворюють триєдиний концептуальний базис побудови систем безпеки. Інформаційна модель оцінювання критичності є ланкою, що пов'язує фізичний чи віртуальний актив із бізнес-контекстом його використання, дозволяючи автоматизувати розрахунок потенційних збитків та трансформувати суб'єктивні судження експертів у чіткі математичні метрики для систем підтримки прийняття рішень у кібербезпеці.

1.2 Огляд міжнародних стандартів та фреймворків категорування активів

Сучасний світовий досвід у сфері кібербезпеки базується на стандартизації процесів ідентифікації та класифікації інформаційних ресурсів. Визначення критичності активів є першим і найбільш відповідальним етапом побудови СБІ. Для забезпечення уніфікації цих процесів провідними міжнародними інституціями розроблено низку нормативно-методологічних документів, що пропонують різні підходи до оцінювання та категорування — від загальних високорівневих фреймворків управління ризиками до спеціалізованих технічних стандартів та вузькогалузевих регламентів.

Міжнародний стандарт ISO/IEC 27005:2022 [11] (впроваджений в Україні як державний стандарт ДСТУ ISO/IEC 27005:2023 [20]) є базовим документом, який визначає філософію та методологічні рамки ризик-орієнтованого підходу. Стандарт не пропонує фіксованої шкали для категорування, а натомість надає гнучкий інструментарій для розробки внутрішньої методики організації. Відповідно до положень стандарту, «критерії оцінювання наслідків мають бути визначені з огляду на цінність активів для організації та її бізнес-цілей» [3, 37]. ISO/IEC 27005 регламентує, що процес визначення критичності активів повинен враховувати не лише прямі фінансові втрати, а й опосередковані наслідки: порушення законодавства, репутаційні збитки, зниження операційної ефективності та загрозу життю або здоров'ю людей. Основною перевагою підходу ISO/IEC 27005 є концепція безперервного моніторингу та переоцінки: критичність активу не є статичною величиною і має динамічно змінюватися у разі трансформації бізнес-контексту чи архітектури ІС [3, 11, 20].

Радикально інший — чітко структурований та інженерний підхід — представлений у федеральних стандартах США FIPS 199, NIST SP 800-30, NIST SP 800-60, розроблених Національним інститутом стандартів і технологій (англ. National Institute of Standards and Technology, NIST).

Базовим документом у цій триаді є Федеральний стандарт обробки інформації FIPS Publication 199 («Standards for Security Categorization of Federal Information and Information Systems») [8]. Стандарт вводить суворе математичне правило для визначення категорії безпеки інформаційного активу або інформаційної системи.

Відповідно до FIPS 199, категорування здійснюється за трьома базовими властивостями безпеки відповідно до моделі CIA (КЦД). Для кожної з властивостей C, I і A визначається рівень потенційного негативного впливу (англ. potential impact), який може бути низьким (Low, *L*), помірним (Moderate, *M*) або високим (High, *H*). Загальна категорія безпеки (SC_{IC}) інформаційної системи формулюється у вигляді математичного виразу [8]:

$$SC_{IC}=\{ Impact_C, Impact_I, Impact_A\}, \quad (1.1)$$

де значення кожного параметра оцінюється за шкалою $\{L, M, H\}$.

Для визначення фінального рівня критичності системи стандарт FIPS 199 застосовує критерій «найгіршого випадку» (правило максимуму), згідно з яким загальний рівень критичності системи дорівнює найвищому значенню серед трьох складових [8]:

$$Total\ Impact = \max(Impact_C, Impact_I, Impact_A). \quad (1.2)$$

Для наочності градацію критеріїв оцінювання рівнів впливу за FIPS 199 наведено у табл.1.1.

Таблиця 1.1 - Матриця оцінювання потенційного впливу за FIPS 199

Складова тріади	Низький рівень впливу (Low)	Помірний рівень впливу (Moderate)	Високий рівень впливу (High)
C	Несанкціоноване розкриття завдає обмеженої шкоди діяльності чи активам	Несанкціоноване розкриття завдає серйозної шкоди діяльності чи активам	Несанкціоноване розкриття завдає катастрофічної шкоди чи загрожує життю
I	Несанкційована модифікація чи знищення завдає обмеженої шкоди	Несанкційована модифікація завдає серйозної шкоди (перебої в роботі)	Модифікація призводить до катастрофічних наслідків або втрати функцій
A	Тимчасова втрата доступу завдає обмеженої шкоди операційній діяльності	Тривала відмова системи завдає серйозної шкоди критичним процесам	Повна відмова системи унеможливлює роботу КІ.

Практичним керівництвом, яке деталізує вимоги FIPS 199 [8], є спеціальна публікація NIST SP 800-60 «Guide for Mapping Types of Information and Systems to Security Categories» (Volume I, Revision 2) [15]. При цьому ризики оцінюються за NIST Special Publication 800-30 «Guide for Conducting Risk Assessments» [14]. Цей документ містить деталізований алгоритм «картування» (mapping) інформаційних систем та типів інформації до відповідних категорій безпеки. Процес категорування за NIST SP 800-60 складається з чотирьох основних етапів:

− ідентифікація типів інформації, що обробляється, зберігається або передається інформаційною системою (використовуючи уніфікований каталог типів інформації, який включає адміністративний, фінансовий, операційний та інші види інформації);

− визначення базових рівнів безпеки (*L, M, H*) для кожного ідентифікованого типу інформації окремо для кожної складової тріади CIA;

− коригування базових рівнів безпеки з урахуванням специфіки функціонування конкретної організації та експлуатаційних умов інформаційної системи (враховуючи фактори агрегації даних, критичних часових рамок або публічності інформації);

− визначення підсумкової категорії безпеки системи на основі інтеграції оцінок усіх типів інформації за правилом максимуму.

Для окремих галузей можуть бути наявні галузеві вимоги категорування, прикладом котрих є уніфіковані вимоги IACS E22 «Computer-based systems» [9], які проаналізовані в п.2.3 даної кваліфікаційної роботи.

Захист ОКІ в Україні здійснюється на підставі міжнародних і вітчизняних нормативно-правових актів, які визначають вимоги до захисту ОКІ та ОКІІ як об’єктів і вимоги щодо забезпечення інформаційної безпеки ОКІІ як ОІД.

Головним нормативним актом Європейського Союзу, який визначає вимоги до захисту ОКІ та ОКІІ як ОІД є «Директива 2022/2555 від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в Союзі, яка вносить зміни до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2)» [4].

1.3 Українська нормативно-правова база категорування

Серед нормативно-правових актів України, які стосуються категорування, мона виділити нормативно правові акти, які стосуються ОКІІ, і нормативно-правові акти, які стосуються всіх активів та ІС.

Основними нормативно-правовими актами, які стосуються ОКІІ, є:

– Закон України «Про основні засади забезпечення кібербезпеки України» [43], прийнятий у 2017 році (остання редакція - 19.10.2025**)**;

– Закон України «Про критичну інфраструктуру» [42], прийнятий у 2021 році (остання редакція - 21.09.2024);

– Стратегія кібербезпеки України. Безпечний кіберпростір - запорука успішного розвитку країни [44], прийнята 26 серпня 2021 року;

– Плани реалізації Стратегії кібербезпеки України, що є рішеннями Ради національної безпеки та оборони і щорічно затверджуються Розпорядженнями Кабінету міністрів України з лютого 2022 року, наприклад «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України» [39];

– Положення про організаційно-технічну модель кіберзахисту, затверджене Постановою Кабінету міністрів України № 1426 у грудні 2021 р.. (остання редакція - 26.12.2024) [40];

– Постанова Кабінету міністрів України №518 від 19.06.2019 «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури» (остання редакція - 20.11.2025) [35];

– Постанова Кабінету міністрів України від 9.10.2020 №943 «Деякі питання об’єктів критичної інформаційної інфраструктури» (остання редакція - 01.01.2026) [17];

– Постанова Кабінету міністрів України «Деякі питання об’єктів критичної інфраструктури» від 9.10.2020 №1109 (остання редакція - 22.05.2026) [18];

– Постанова Кабінету міністрів України від 13.11.2025 № 1470 «Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. №518» [34];

– Наказ Адміністрації Держспецзв’язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту» [36].

Методичною основою забезпечення захисту всіх активів та ІС, в яких «обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» є НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» [30].

1.4 Порівняльний аналіз існуючих програмних засобів оцінювання ризиків та обґрунтування необхідності автоматизації процесу категорування

Для практичної реалізації ризик-орієнтованого підходу та виконання вимог національного законодавства щодо категорування активів організації використовують спеціалізоване програмне забезпечення. Сучасний ринок пропонує широкий спектр систем класу GRC (англ. Governance, Risk, and Compliance — Управління, ризики та відповідність вимогам) та IRM (англ. Integrated Risk Management — Інтегроване управління ризиками), які дозволяють автоматизувати процеси ідентифікації, оцінювання та моніторингу інформаційних ресурсів [5, 16].

Якісний і кількісний аналіз та моделювання системи ризиків є тими інструментальними засобами, які дозволяють виокремити суттєві ризики з несуттєвих і визначити пріоритети обробки ризиків. Їх реалізація передбачає здобуття відповідної експертної інформації. Методи експертних оцінки включають комплекс логічних і математико- статистичних методів і процедур, пов’язаних з діяльністю експерта по переробці необхідної для аналізу і прийняття рішень інформації. Можна виділити наступні основні методи експертних оцінок, що застосовуються для аналізу ризиків, які, зокрема, вказані в ICE/ISO 31010 і ДСТУ ICE/ISO 31010:

- запитальники; SWOT-аналіз;
- роза і спіраль ризиків;
- оцінка ризику стадії проекту;

– метод Дельфі та інші.

Існують автоматизовані методики оцінки ризиків, які не пов’язані з конкретним програмним засобом і методики, реалізовані у вигляді програмних продуктів. Серед останніх слід виділити:

– метод CRAMM (CCTA Risk Analysis and Management Method, розробник – CCTA, Великобританія) реалізований фірмою Insight Consulting Limited в однойменному програмному продукті. Програмний засіб CRAMM для кожної групи ресурсів (і кожного з 36 типів загроз) генерує список запитів, для яких після ініціалізації даних оцінювання рівнів здійснюється, наприклад, як – дуже високий, високий, середній, низький, дуже низький (для загрози), і як – високий, середній та низький (для уразливості). Загрози та уразливості об'єднуються в матриці ризику, і проводиться аналіз ризиків оцінка ризику. Під час аналізу пропонується виставити коефіцієнти для кожного ресурсу з точки зору частоти виникнення загрози та ймовірності її реалізації. Виходячи з оцінок вартості ресурсів ІС, що захищається, загроз та уразливостей, визначаються «очікувані річні втрати», які переводяться в бали за прийнятою шкалою і показують розраховані ризики. За цими ризиками визначаються оцінки ризиків: певні діапазони оцінок наперед відносять, наприклад, до «дуже низьких», «низьких» і так далі ризиків;

– методику COBRA (Consultative Objective and Bi-Functional Risk Analysis, розробник – C & A Systems Security Ltd, Великобританія) орієнтовану на підтримку вимог стандарту ISO 17799 за допомогою тематичних опитувальників. У комплект ПЗ входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst і COBRA Data Protection Consultant, а також менеджер модуля COBRA, який використовується для налагодження та зміни бази знань. На основі ініціалізації тематичного опитувальника (ТО) здійснюється аналіз ризиків за декількома категоріями: високорівнева безпека; оперативна безпека, безпека електронної комерції тощо. Після обробки ініціалізованих даних система генерує звіт, в якому описана

детальна оцінка за такими характеристиками ризику як категорія, рівень, оцінка. COBRA оцінює відносну важливість усіх загроз і вразливостей, автоматично пов'язує виявлені ризики з потенційними наслідками для бізнес-одиниці;

– метод EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité, розробник Національне агентство комп'ютерної безпеки (ANSSI), Центральне управління безпеки інформаційних систем (DCSSI), Франція) відображає вимоги стан-дартів ISO/IEC 27001, ISO 31000 та ISO/IEC 27005. Процес аналізу та оцінювання ризику реалізується за допомогою п'яти модулів;

– систему RiskWatch (розробник – компанія RiskWatch, США) відображає вимоги стандартів ISO/IEC 27001 та ISO/IEC 27002, NIST а також COBIT IV. Процес аналізу та обробки ризиків проводиться за чотири фази. За аналогією з ПЗ COBRA в RiskWatch для спрощення введення та обробки даних застосовуються тематичні опитувальники та вибір відповіді (даних) з набору варіантів. За допомогою запитів відображаються та оцінюються поточні правила ІБ відповідно до існуючих стандартів. В RiskWatch містяться вбудовані бази статистичних даних, які описують регіональні характеристики загроз, і бази різних систем захисту інформації. Ефект від впровадження засобів безпеки визначається параметром ROI – повернення інвестицій, що складає прибуток від вкладень за період часу;

– інструментарій RA2 art of risk (RA Software Tool, розробник – компанії AEXIS Security Consultants та XiSEC Consultants Ltd., Великобританія) є ПЗ для реалізації СМІБ, відповідно до вимог ISO/IEC 27001: 2005 і складається з восьми модулів. В процесі виконання кожного модуля проводиться ініціалізація запитів за допомогою вибору фіксованих значень в бінарно-лінгвістичній формі («так», «ні»). Лінгвістична шкала оцінок ризиків має 5 градацій: тривіальний; мінорний; значний; великий; катастрофічний;

– інструментарій PTA (Practical Threat Analysis, розробник PTA Technologies, Ізраїль) заснований на вимогах стандарту ISO/IEC 27001 та PCI

DSS 1.1 і є програмною системою для розробки моделі загроз, оцінювання ризиків ІБ та складання планів щодо їх зниження. Всі перераховані процеси реалізуються за допомогою чотирьох кроків від ідентифікації ресурсів, кожному з яких присвоюється певний ідентифікатор (наприклад А003) до розробки планів нейтралізації сценаріїв загроз;

– КЕС управління ІБ «Авангард» (Комплексна експертна система «Авангард», розробник – Лабораторія системного аналізу проблем інформатизації Інституту системного аналізу РАН, Росія) включає комплекс методик і базується асновується на двох програмних комплексах – «Авангард-Аналіз» і «Авангард-Контроль». Для кожної одиниці ризику встановлюється грошовий еквівалент;

– систему Enterprise Risk Assessor (Risk Advisor, розробник – компанія Methodware, Нова Зеландія), яка відповідає вимогам австралійського стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360: 1999) та ISO/IEC 17799. Представлена в трьох продуктах: CobiT Advisor 3rd Edition (Audit); PRo Audit Advisor; Planning Advisor. Після побудови моделі формується звіт (близько 100 розділів) та агрегований опис у вигляді графа ризиків. У звіті з ймовірносно-лінгвістичною шкалою ризик представляється у вигляді матриці з такими градаціями: майже напевно, ймовірно, можливо, малоймовірно, рідко;

– систему vsRisk, Risk Assessment Tool (розробник – компанія Vigilant Software Ltd., Великобританія), яка призначена для аналізу ризиків ІБ відповідно до вимог ISO/IEC 27001 та BS 7799-3. Для спрощення процедури використовуються форми, для яких вибираються шкали (встановлюються рівні) ймовірності та впливу. Далі, для кожної дії визначається ймовірність за обраною шкалою. Система надає засоби для оцінки всіх чинників ризиків, включаючи загрози, уразливості, активи та механізми контролю, і не містить засобів для кількісної оцінки величини ризику, обмежуючись лише якісними шкалами;

– систему OCTAVE (Operationally critical threats, assets and vulnerability evaluation, розробник – інститут Carnegie Mellon Software Engineering Institute і Центр навчання, досліджень і технологій (CERT)), яка реалізована в лінійці продуктів: метод OCTAVE, OCTAVE-S та OCTAVE Allegro – для великих, середніх і малих організацій відповідно, США). Система призначена для виконання математичних розрахунків, для чого надає інтерпретовану мову, багато в чому сумісну з Matlab. OCTAVE можна використовувати для пакетної обробки. Мова OCTAVE має розширення для розв'язування лінійних і нелінійних алгебраїчних та диференціальних рівнянь, до яких можна додавати динамічно завантажувані модулі, створені на мовах C, C++, Фортран та ін.). В основний склад OCTAVE включені також пакети для інтеграції з мовою Java;

– інструментарій Callio Secura 17799 (розробник – компанія Callio Technologies, Канада) є Web-додатком, який включає все необхідне для менеджера при розробці, впровадженні, управлінні та сертифікації СМІБ згідно ISO/IEC 17799 / BS7799. Система містить чотири секції («Методологія», «Адміністрування», «Інструменти» та «Управління ІБ») і використовує тематичні опитувальники. При аналізі ризиків визначаються збитки, що є наслідками порушення конфіденційності, цілісності, доступності;

– систему «Гриф 2006» (розробник – компанія Digital Security, Росія) спрямовану на забезпечення самостійної роботи IT-менеджера (без залучення сторонніх експертів) щодо оцінки ризиків. Аналіз ризиків здійснюється за допомогою побудови моделі ІС організації. Ризик оцінюється окремо за кожною зв'язкою «група користувачів – інформація», тобто модель розглядає взаємозв’язок «суб'єкт – об'єкт» з урахуванням всіх їх характеристик. Конфігурація звіту, який генерує «Гриф 2006», може бути практично будь-якою, таким чином, дозволяючи створювати як короткі звіти для керівництва, так і детальні звіти для подальшої роботи з результатами;

– систему @RISK (розробник – компанія Palisade, США), яка призначена для аналізу і обробки ризиків за допомогою методу Монте-Карло, що

реалізується на основі Microsoft Excel. Система дозволяє простежити можливість прийняття та уникнення ризиків, а також приймати найкращі рішення в умовах невизначеності. Для оцінки ризиків також використовується метод Value at Risk (VAR);

– систему RiskPAC (розробник – компанія CSCI, Нідерланди), яка призначена для виявлення та надання допомоги в усуненні уразливостей в ІС. Конструктор анкет дозволяє автоматизувати будь-яку ручну методику шляхом ініціалізації (за допомогою фіксованих варіантів) запитів в тематичних опитувальниках,, представлених у вигляді реляційних баз даних. Ймовірності оцінюються за шкалою з трьома градаціями (малоймовірно, ймовірно та цілком ймовірно), а негативний вплив – за шкалою з чотирма градаціями (мінімальний, значний, серйозний та катастрофічний). Додатково в системі є калькулятор очікуваних середньорічних втрат;

– систему Microsoft Security Assessment Tool (MSAT, розробник – компанія Microsoft, США), яка орієнтована на організації з числом співробітників менше 1000 осіб. для сприяння кращому розумінню потенційних проблем у сфері ІБ. В ході роботи користувач, який виконує роль аналітика, працює з двома групами запитів, перша з яких присвячена оцінюванню ризиків для бізнесу, з яким компанія стикається в даній галузі та в умовах обраної бізнес-моделі (творюється так званий профіль ризику для бізнесу). Після цього здійснюється дистанційна обробка (через Інтернет) отриманої інформації та перехід до другої групи запитів, які організовані відповідно до концепції багаторівневого (ешелонованого) захисту інформації. Використовується тематичний опитувалник, що відповідає розділам стандартів ISO/IEC 17799 та ISO/IEC 27001. Негативні наслідки і частоти виникнення загроз оцінюються за трирівневими шкалами. Після ініціалізації запитів клієнтська частина програмної системи знову звертається до віддаленого сервера та генерує звіти, зокрема - «Повний звіт», що містить пропонований список пріоритетних дій;

– методику TRA (Threat and Risk Assessment, розробник – компанія Government (Communications Security Establishment), Канада), розроблену на основі трьох посібників для IT-систем з: сертифікації та акредитації (MG-01); управління ризиком безпеки (MG-02); оцінювання ризиків і вибору гарантій (MG-03). Оцінка ризиків здійснюється після опису аналітиком для кожної загрози її сценаріїв сценаріїв фільтрації. Рівень порушення таких характеристик як К, Ц та Д оцінюється за трирівневою шкалою;

– методику FRAP (Facilitated Risk Analysis Process, розробник – компанія Peltier and Associates, США), яка розглядає інформаційну безпеку ІС в рамках процесу управління всіма ризиками організації та складається з п'яти етапів. Оцінка здійснюється у відповідності з правилом, яке задається матрицею ризиків і може інтерпретуватися наступним чином: рівень А – заходи з обробки ризику повинні бути виконані негайно і в обов'язковому порядку; рівень В – заходи з обробки ризику мають бути вжиті; рівень С – потрібний моніторинг ситуації; рівень D – ніякі заходи в даний момент не потрібні. Отримані результати детально документуються в стандартизованому форматі;

– методику Risk Matrix (розробник компанія Mitre Corporation, США), яка орієнтована на аналіз та обробку ризиків і згодом була реалізована додатком для Microsoft Excel. Спочатку проводиться ідентифікація ризику за допомогою застосування експертами «Мозкового штурму». Далі присвоюються різні атрибути кожному ризику, такі як, наприклад, період часу (дати початку і закінчення можливої реалізації) та ймовірності виникнення. За допомогою сценарію «Якщо ризик ..., то наслідки ...» складається матриця ризику. Для визначення найбільш пріоритетних ризиків використовується діаграма частот;

– методлогію Mehari (розробник Clusif, Франція), яка інтегрує інструменти (наприклад, критерії оцінки, формули та ін.) і бази знань (зокрема, заходи для діагностики кібербкзпеки), що є важливим доповненням до мінімальних методів запропонованих в ISO/IEC 27005. Для оцінки ризику

пропонуються два основні варіанти – використання баз знань (які інтегруються в Microsoft Excel, Open Office) або ПЗ (наприклад, Risicare, яке забезпечує більш багатий користувальницький інтерфейс, а також дозволяє моделювати, візуалізувати та оптимізувати отримані результати);

– методику MAGERIT (Methodology for Information Systems Risk Analysis and Management, розробник Ministerio De Administraciones Públicas, Іспанія), в якій при оцінюванні негативності наслідків реалізації загроз для кожного інформаційного ресурсу визначається у відсотках вплив загроз на конфіденційність, цілісність та доступність даних, справжність користувача послуг, походження даних, підзвітність використання послуг і доступу до даних;

– методику Information Security RA (Risk Assessment, розробник Centers for Medicare & Medicaid Services (CMS), США), яка складається з 3-х фаз: документування системи, визначення ризику. Оцінювання ступенів впливу загрози на систему (впливу, який загроза матиме на дані і бізнес-функції ІС з точки зору втрати К, Ц і Д) здійснюється за шестирівневою шкалою, а визначення ймовірності її виникнення з урахуванням наявних елементів управління – за семирівневою шкалою;

– PILAR (Environment for the Analysis of Risk, розроблена під егідою Національного криптологічного центру Іспанії) безпосередньо реалізує методику Magerit та стандарти безпеки НАТО, фокусуючись на детальному картуванні зв'язків між активами та загрозами. PILAR дозволяє ідентифікувати активи, оцінювати загрози й вразливості, розробляти плани вдосконалення безпеки та розраховувати залишкові ризики після впровадження контрзаходів;

– платформа Axonius (розробка одноіменної компанії, Ізраїль) використовує аналітичні дані на базі штучного інтелекту, розширену мережу інтеграції та можливості автоматизації, щоб забезпечити командам безпеки та IT єдину модель даних про активи, яка дозволяє вживати проактивних

заходів безпеки в масштабах. Axonius забезпечує комплексну видимість та дієвість щодо кіберактивів, SaaS-додатків, програмного забезпечення, ідентифікаційних даних, ризиків та інфраструктури — все в єдиному об'єднаному вигляді. Інтегруючи дані з понад тисячі джерел, платформа допомагає організаціям зменшити складність та вживати заходів за допомогою автоматизованого реагування та виправлення. Інтегрована платформа об'єднує дані з кожної системи IT-інфраструктури організації для оптимізації критично важливих показників ризиків, продуктивності та витрат за допомогою дієвої аналітики. Axonius зміцнює кіберстійкість, забезпечуючи видимість активів для передбачення, протистояння та відновлення після інцидентів безпеки [2];

– Armis (розробник – компанія Armis Security, США) - хмарна AI-платформа кібербезпеки та управління кіберризиками, створена для захисту всіх типів активів та керування поверхнею атак в режимі реального часу. Вона забезпечує повну видимість мережі та захищає як керовані, так і некеровані пристрої і охоплює традиційні IT-пристрої, Інтернет речей (IoT), операційні технології, медичні прилади, хмарні середовища та системи штучного інтелекту Armis працює без встановлення агентів на кінцеві пристрої, використовуючи пасивний моніторинг трафіку та інтеграцію з наявними мережевими системами, проактивно сканує середовище, виявляє вразливості, відстежує поведінку та блокує кіберзагрози [1];

– IT Risk Manager (ITRM, розробники - компанія TechExpert і Агентство Активного Аудиту, Україна). Це комплексна українська система для автоматизації управління ризиками інформаційної безпеки. Вона дозволяє оцінювати активи, формувати перелік можливих загроз, обчислювати рівні ризиків та розробляти заходи для їх зниження відповідно до стандартів серії ISO/IEC 27000. Рішення реалізовано на базі програмного забезпечення з відкритим вихідним кодом GLPI і являє собою готовий інструмент для оцінки та обробки ризиків інформаційних активів компанії.

Для роботи з системою не потрібне встановлення додаткових клієнтських додатків, достатньо наявності будь-якого сучасного браузера.

Архітектура цих систем, їхня функціональність та орієнтація на конкретні правові поля суттєво відрізняються, що вимагає розробки чітких критеріїв для їх порівняльного аналізу.

Проведений аналіз ринку програмного забезпечення дозволяє виділити три основні класи автоматизованих систем, що використовуються для оцінювання критичності та ризиків ІС:

– глобальні корпоративні GRC-платформи - масштабні системи, призначені для великих підприємств, які інтегрують управління ІТ-ризиками з операційними та фінансовими ризиками компанії;

– інструменти аналізу кіберризиків для експертів з інформаційної безпеки (PILAR, Cramme) [5];

– платформи управління кібер-активами (Axonius, Armis). Сучасний клас систем, які здійснюють автоматичний збір даних про наявні пристрої, програмне забезпечення та інформаційні потоки в мережі організації в режимі реального часу, виявляючи так зване «Shadow IT» [1, 2].

Для об'єктивного оцінювання та вибору програмних засобів оцінювання критичності інформації та ІС було сформовано п'ять ключових критеріїв:

– К1: Рівень автоматизації збору даних про активи;

– К2: Підтримка національної нормативної бази України;

– К3: Наявність математичного апарату обробки невизначеності;

– К4: Здатність враховувати каскадний ефект (моделювати залежності);

– К5: Вартість впровадження та доступність для українського ринку (враховує ціну ліцензій, складність розгортання та залежність від хмарних сервісів країн-виробників в умовах обмежень воєнного стану).

Результати порівняльного аналізу провідних програмних комплексів за визначеними критеріями наведено у табл. 1.2.

Таблиця 1.2 - Порівняльний аналіз провідних програмних засобів оцінювання ризиків та критичності ІС

Програмний засіб / Платформа	К1: Автоматизація збору	К2: Нормативна база UA	К3: Математичний апарат	К4: Каскадний ефект	К5: Доступність / Вартість
ServiceNow IRM	Високий (через модуль Discovery / CMDB)	Відсутня (орієнтація на NIST, GDPR, ISO)	Низький (лінійні матриці ризиків)	Середній (статичні зв'язки в CMDB)	Дуже низька (екстремально висока вартість)
PILAR (Magerit)	Низький (виключно ручне введення / імпорт)	Відсутня (підтримка стандартів ENISA, NATO)	Середній (якісно-кількісні шкали)	Високий (дерева залежностей активів)	Середня (ліцензування для державних установ)
Axonius	Дуже високий (пасивний та активний сканінг)	Відсутня (базові технічні метрики)	Відсутній (немає блоку оцінки збитків)	Низький (бачить лише мережеві зв'язки)	Низька (висока вартість, підписочна модель)

Аналіз інструментів оцінювання ризиків та критичності ІС показує, що закордонні системи фокусуються на візуалізації процесу та лінійному розрахунку ризиків.

Розглядаючи інтерфейси та логіку роботи класичних GRC-систем (наприклад, RSA Archer), можна помітити, що процес категорування та оцінки наслідків реалізується через заповнення статичних опитувальників та автоматичне формування матриць ризиків розмірністю 3×3 або 5×5. Такі інтерфейси, попри свою наочність, мають суттєвий методологічний недолік: вони не відображають динамічну зміну архітектури ІС та змушують експертів вручную обирати рівні збитків («обмежена шкода», «серйозна шкода»), що вносить суттєвий суб'єктивізм у підсумковий результат.

У свою чергу, спеціалізовані системи аналізу ризиків, такі як PILAR, використовують більш просунуті інтерфейси картування активів, де користувач будує ієрархічні дерева залежностей: «Бізнес-процес → Інформаційна система → Сервер → Мережевий комутатор → Інформаційний ресурс (актив)». Проте ручне заповнення таких профілів для організації з тисячами активів

перетворюється на надскладне завдання, яке швидко втрачає актуальність через постійні зміни в ІТ-середовищі.

Викладене вище обґрунтовує гостру необхідність автоматизації процесу категорування та розробки спеціалізованої інформаційної моделі в межах даної кваліфікаційно роботи, що підтверджується такими чинниками:

– динамічність та масштабність сучасних ІС. Кількість інформаційних ресурсів в організаціях зростає експоненціально. Проведення оцінювання критичності «вручну» за допомогою паперових анкет або таблиць Excel, як це часто практикується під час виконання вимог НД ТЗІ 3.6-005-21, займає місяці та застаріває на момент підписання акту комісії;

– невідповідність зарубіжного ПЗ вимогам України. Жодна з існуючих світових GRC-систем не підтримує специфіку українського законодавства у сфері технічного захисту інформації та кіберзахисту об'єктів критичної інфраструктури. Вітчизняні підприємства змушені або використовувати непідтримувані моделі, або розробляти власні рішення;

– врахування прихованих зв'язків (каскадування). Лише автоматизований алгоритм здатний прорахувати ланцюгову реакцію, коли компрометація умовно «некритичного» активу (наприклад, шлюзу збору телеметрії) через мережеві залежності призводить до деградації системи вищого рівня безпеки, що є критично важливим для транспортної та енергетичної галузей.

Висновки до розділу 1

Порівняльний аналіз розглянутих міжнародних стандартів дозволяє зробити висновок, що найбільш математично формалізованим та придатним для автоматизації в межах кваліфікаційної роботи є підхід інституту NIST (FIPS 199 / NIST SP 800-60). Проте його пряме копіювання є неможливим через

відсутність гнучкості при аналізі складних внутрішніх взаємозв'язків між системами.

Концепція «найгіршого випадку» (максимального впливу) часто призводить до штучного завищення критичності допоміжних систем, що тягне за собою надлишкові фінансові витрати на захист. Це обумовлює необхідність розробки нової, більш збалансованої інформаційної моделі, яка б поєднувала структурну чіткість стандартів NIST, ризикову гнучкість ISO/IEC 27005 та враховувала специфіку категорування складних об'єктів автоматизації, описану в галузевих стандартах типу IACS UR E22.

Проведений аналіз дозволив виявити наступні недоліки існуючих підходів до оцінки критичності інформаційних систем:

– статичність: оцінки проводяться періодично, а не в реальному часі, що робить їх неефективними проти динамічних кіберзагроз. Традиційні експертні методи оцінювання ризиків, що виконуються дискретно (наприклад, один раз на рік), швидко втрачають актуальність;

– фрагментарність: розгляд систем ізольовано без врахування міжсекторальних взаємозв’язків та ланцюжків постачання. Потрібно враховувати каскадний ефект;

– суб'єктивність: надмірна залежність від експертних оцінок, що ускладнює автоматизацію та стандартизацію.

– фокус на ресурсах, а не на функціях: оцінка захищеності окремих серверів замість здатності системи виконувати свої критично важливі послуги в умовах атак

– неузгодженість категорій і рівнів критичності, що визначаються за різними нормативними документами і є чинними на одному ОІД.

Таким чином, проведений аналіз понятійного апарату, міжнародних стандартів, національного законодавства та існуючих програмних засобів підтвердив, що попри наявність розвиненої теоретичної бази, практична реалізація процесів категорування інформаційних систем в Україні стримується

відсутністю адаптованих, гнучких та автоматизованих інструментів. Існуючі зарубіжні аналоги є недоступними за вартістю та не враховують вимоги нормативних документів ДССЗЗІ (зокрема НД ТЗІ 3.6-005-21). Це повністю обґрунтовує актуальність, мету та завдання кваліфікаційної роботи, спрямованої на розробку інформаційної моделі та алгоритмів для автоматизованого оцінювання критичності інформаційних активів установи.

РОЗДІЛ 2. ФОРМАЛІЗАЦІЯ ТА МОДЕЛЮВАННЯ ПРОЦЕСУ ОЦІНЮВАННЯ КРИТИЧНОСТІ АКТИВІВ

2.2 Категоризація об’єктів критичної інфраструктури

Категорія критичності визначається для ОКІ, ОКІІ та ІС у послідовності, наведеній на рис.2.1.

Рисунок 2.1 – Послідовність визначення категорій критичності

Прешим кроком при цьому є визначення ОІД як ОКІ відповідно до спектру основних послуг, що надаються цим об’єктом.

Наступним кроком є визначення для ОКІ секторальних критеріїв оцінювання критичності. Наприклад, морський і внутрішній водний транспорт та суднобудування за Постановою Кабінету міністрів України №1109 (в редакції 26-го року [18]):

– є підсекторами різних секторів КІ України;

– мають різні секторальні органи у сфері захисту КІ;

– надають різні основні послуги;

– мають однакову кількість міжсекторальних критеріїв оцінювання рівнів критичності ОКІ – 15;

– мають однакову кількість секторальних критеріїв оцінювання рівнів критичності ОКІ – 1, які різняться за змістом (табл.2.1, табл.2.2);

– мають однакову максимальну сумарну оцінку рівнів критичності $\Sigma PK_{\max}$.

Таблиця 2.1 – Порівняння підсекторів КІ «Морський та внутрішній водний транспорт» та «Суднобудування»

Характеристики	Морський та внутрішній водний транспорт	Суднобудування
Сектор	Транспорт і пошта	Промисловість
Секторальний орган у сфері захисту КІ	Міністерство інфраструктури (Мінінфраструктури)	Міністерство з питань стратегічних галузей промисловості України (Мінстратегпром)
Основні послуги	– здійснення контролю та нагляду за безпекою судноплавства та мореплавства; – інжинірингова діяльність для будівництва, ефективного використання та утримання об'єктів портової інфраструктури, розташованих у межах території та акваторії морського порту; – обслуговування суден, що заходять до морських, річкових портів (терміналів) України, пасажирів, вантажів (вантажно-розвантажувальні роботи, обслуговування, зберігання, перевезення вантажів, пасажирів); – обслуговування та утримання внутрішніх водних шляхів, об'єктів інфраструктури внутрішнього водного транспорту; –виконання міжнародних зобов'язань України у тому числі: –лоцманське проведення суден –регулювання руху суден; –технічний нагляд за суднами; –пошук і рятування людей в морі; – гідрографічне забезпечення.	суднобудування та постачання продукції суднобудування
Кількість міжсекторальних критеріїв оцінювання рівнів критичності ОКІ	15	15
Кількість секторальних критеріїв оцінювання рівнів критичності ОКІ	1 «Знищення, пошкодження або порушення функціонування ОКІ призведе до ненадання об'єктом основних послуг»	1 «Знищення, пошкодження або порушення функціонування ОКІ призведе до ненадання об'єктом основних послуг»
Максимальна сумарна оцінка рівнів критичності $\Sigma PK_{\max}$	68	68

Таблиця 2.2 – Секторальні критерії оцінювання критичності ОКІ в підсекторі «Морський та внутрішній водний транспорт» сектору «Транспорт і пошта» та в підсекторі «Суднобудування» сектору «Промисловість»

Фактор негативного впливу в підсекторі	Критерій оцінювання негативного впливу			
	Умова		Рівень негативного впливу	Оцінка $РК_i$
	«Морський та внутрішній водний транспорт»	«Суднобудування»		
Знищення, пошкодження або порушення функціонування ОКІ призведе до ненадання об’єктом основних послуг	не застосовується	для менш як 6000 жителів	незначні наслідки	1 бал
	час припинення надання морських послуг у морських портах може становити не більше як 24 години	для більш як 6000 жителів	значні наслідки	2 бала
	час припинення надання морських послуг у морських портах може становити від 24 до 72 годин	для більш як 30 000 жителів на території області або більш як одного району міста - обласного центру, або на всій території одного міста обласного значення	критичні наслідки	3 бали
	припинення надання морських послуг у морських портах більш як на 72 години (Правила надання послуг у морських портах України, затверджені наказом Мінінфраструктури від 5 .06.2013 р. № 348)	для більш як 100 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення	катастрофічні наслідки	4 бала

Міжсекторальні критерії оцінювання критичності ОКІ є однаковими для всіх секторів і підсекторів і визначаються за різними показниками і умовами (за потенційною кількістю смертельних випадків, значимістю можливих економічних втрат, рівнем негативного впливу на суспільну довіру, критичністю екологічних наслідків, впливом на інші сектори КІ тощо), які дозволяють оцінити критичність порушення функціонування ОКІ для соціуму і держави.

Категорія критичності присвоюється ОКІ згідно Закону України «Про критичну інфраструктуру» [42] спеціальною робочою групою експертів, створеною в межах сектора або підсектора. Категорія критичності є якісною експертною оцінкою діапазону, до якого належить розрахована за секторальними і міжсекторальними критеріями узагальнена нормована оцінка критичності $РК_{ОКІ}$.

Для кожного ОКІ, згідно із методикою категоризації ОКІ [34, 37], робочою групою в межах її відповідальності за всіма m критеріями визначаються експертні оцінки його критичності $РК_i$ (дискретні оцінки від 0 до 4 балів) і розраховується узагальнена нормована оцінка критичності $РК_{ОКІ}$ за формулою:

$$PK_{OKI} = \frac{\sum_{i=1}^{m} PK_i}{\sum_{i=1}^{m} PK_{i\_\max}}. \qquad (2.1)$$

За діапазоном значень, в який потрапляє $РК_{ОКІ}$, ОІД може бути присвоєна одна із чотирьох категорій критичності:

− якщо $0{,}8 < РК_{ОКІ} \leq 1$, то - І категорія критичності (ОІД є ОКІІ і є особливо важливим;

− якщо $0{,}63 < РК_{ОКІ} \leq 0{,}8$, то - ІІ категорія критичності (ОІД є ОКІІ і є життєво важливим);

− якщо 0,37<$РК_{ОКІ}$≤0,63, то - III категорія критичності (ОІД є ОКІІ і є важливим);

− якщо 0,2<$РК_{ОКІ}$≤0,37, то - IV категорія критичності (ОІД є ОКІІ і є необхідним);

− якщо $РК_{ОКІ} \leq 0,2$, то ОІД не є критичним і не є ОКІІ

Критичність об'єктів інформаційної інфраструктури, які входять до складу ОКІ, визначається за окремими правилами:

а) якщо кібератака на комунікаційну або технологічну систему об'єкту інформаційної інфраструктури ОКІ впливає на стале функціонування ОКІ і виконання ним основних функцій, то цей об'єкт (за Законом України «Про основні засади забезпечення кібербезпеки України» [43]) є ОКІІ ОКІ;

б) ОКІІ присвоюється та ж сама категорія критичності, що й ОКІ в разі виконання всіх умов, які визначені в «Порядку формування переліку об'єктів критичної інформаційної інфраструктури», затвердженому Постановою Кабінету Міністрів України від 9 жовтня 2020 р. №943 [17]):

− ОІД є необхідними для стійкого надання ОКІ основних послуг;

− інцидент з інформаційної безпеки на ОІД істотно впливає на безперервність та стійкість надання ОКІ основних послуг;

− відсутній альтернативний спосіб надання ОКІ тих послуг, що надає даний ОІД.

2.2 Категоризація інформації та інформаційних систем за НД ТЗІ 3.6-004-21

За НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [29] процес впровадження СБІ містить етап категоріювання безпеки. Нв цьому етапі має

бути оцінена критичність порушення властивостей КЦД для всіх активів ІС, визначена критичність активівв та ІС в цілому.

Порядок оцінювання критичності інформації, активів та ІС встановлюються НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» [30]. Згідно з цим документом в процесі категоріювання виконуються три завдання:

− К-1. Опис інформаційної системи;

− К-2. Категоріювання безпеки;

− К-3. Аналіз і ухвалення рішення за результатами категоріювання безпеки ІС та інформації.

Кожне завдання має низку підзадач, зокрема підзадачами завдання К-2 є:

Підзадача К-2.1. Визначення рівнів критичності інформації, що обробляється в ІС і асоційована з певним активом. Рівні критичності (*РК*) визначаються окремо за ступенем потенційних збитків (рівнями негативного впливу), які можуть спричинити порушення конфіденційності, цілісності та доступності інформації. Вони визначаються як якісні показники: $РК \in$ {Низький, Середній, Високий}. В результаті для кожного *j*-го активу отримують множину $\{РК_{j,\text{ конфіденційність}}, РК_{j,\text{ цілісність}}, РК_{j,\text{ доступність}}\}$.

Підзадача К-2.2. Визначення рівнів критичності активів ІС за правилом:

$$РКr_j = \max(РК_{j,\text{ конфіденційність}}, РК_{j,\text{ цілісність}}, РК_{j,\text{ доступність}}). \qquad (2.2)$$

При наявності множини з *J* активів $A=\{IA_j\}$, $j = \overline{1, J}$ отримуємо множину оцінок їх рівнів критичності $РКА=\{РКr_j\}$.

Підзадача К-2.3. Визначення рівня критичності ІС за правилом:

$$РК_{IC} = \max(РКr_j), \qquad (2.3)$$

тобто $РК_{IC}$ визначається як максимальний *РК* серед усіх інформаційних активів ІС.

2.3 Категорризація інформаційних систем за IACS UR E22

Згідно уніфікованих вимог Міжнародної асоціації класифікаційних товариств IACS UR E22 «Computer-based systems» [9] категорія критичності комп'ютеризованої системи, яка в морській галузі є за змістом аналогічною терміну «інформвційна система» з НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» [30], визначається за тяжкістю наслідків виходу ІС з ладу (табл.2.3). Тяжкість наслідків оцінюється з точки зору безпеки людини, судна (його живучрсті) та/або до загрози для навколишнього середовища.

Таблиця 2.3 – Категорії критичності суднових комп'ютеризованих систем

Категорія	Негативні наслідки:	Типова функціональність систем
I	Відсутні	Моніторинг, інформаційна та адміністративна функції
Категорія	Негативні наслідки:	Типова функціональність систем
II	Можливі	Суднова тривога, функції моніторингу і управління, які необхідні для підтримки судна в нормальному стані для експлуатації та проживання
III	Зявляються негайно	Управління рухом судна, рульове керування, функції безпеки судна

IACS UR E22 регламентує вимоги до проектування, тестування та експлуатації комп'ютеризованих систем, що використовуються на суднах та об'єктах морського транспорту (і активно адаптується для залізничного транспорту в межах загальноєвропейських систем безпеки) [9].

Сучасна редакція стандарту IACS UR E22 (Rev.3) суттєво розширює вимоги до кібербезпеки цих систем, зазначаючи, що «для систем Класу II та Класу III має бути проведено повний аналіз вразливостей та оцінку критичності програмного забезпечення з метою запобігання несанкціонованому зовнішньому впливу» [9]. Це підтверджує світову тенденцію до злиття вимог інформаційної безпеки традиційних систем автоматизації технологічних

процесів та класичних інформаційних технологій (IT) в єдину інформаційну модель захисту.

Системи категорії I не є небезпечними і не перевіряються Класифікаційним товариством, якщо документально зафіксовано (як відповідь на запит Класифікаційного товариства), що вони не впливають на роботу систем категорії II та III.

Категорії оцінюються в контексті, тому категорії однієї й тієї ж комп’ютертзованої системи на різних суднах можуть бути різними.

IACS UR E22 є чинними для всього життєвого циклу суднових комп'ютеризованих систем, які для виконання свої функцій використовують програмне забезпечення, окрім систем, вимоги до яких регулюються іншими нормативними актами. IACS UR E22 застосовуються до систем управління, сигналізації, моніторингу, забезпечення безпеки і внутрішнього зв'язку судна, які підлягають класифікаційним вимогам. IACS UR E22 не застосовуються, наприклад, до навігаційних систем і радіо-комунікаційних систем (бо вони регулюються главами V і IV SOLAS).

Результати всіх процесів категоризації оформлюються у вигляді акту категоризації.

2.4 Пропозиції науковців щодо категоризації інформації та інформаційних систем

В тезах [47] розроблені пропозицій до удосконалення процедур категоризації об'єктів критичної інфраструктури шляхом врахування нечіткості оцінок РКі, наданих експертами. Доцільність такого підходу зумовлена тим, що, по-перше, хоча оцінка за кожним критерієм $РК_i$ згідно [34, 37] визначається експертом як чітке число, однак підставою для визначення оцінок для окремих критеріїв є належність певного кількісного показника до визначеного в нормативних документах числового діапазону, який за змістом відповідає

носію нечіткої множни. По-друге, експерт може не бути впевнений на 100% у належності кількісного показника тільки одному діапазону. Для обєктивного віддзеркалення експертних оцінок критичності ОІД за секторальними і міжсекторальними критеріями в [47] пропонується використовувати оцінку, зважену за мірами впевненості експертів. В [47] оцінені накопичені за всіма критеріями похибки, зумовлені тим, що міри впевненості експерта в конкретній бальній оцінці негативних наслідків $\mu_i \neq 1$.

В роботі [24] «запропоновано узагальнену модель системи характеристик даних, в якій на підставі застосування теоретико-множинного підходу за рахунок побудованих множин категорій» створюється підгрунття для формалізації «оцінювання поточного стану кіберзахисту об'єкта критичної інформаційної інфраструктури України».

У статті [13] пропонується підхід, заснований на використанні систем нечіткої логіки для оцінки ризиків багатоетапних кібератак на мережеві операційні служби. Запропонована методологія враховує неоднозначність та розмитість вхідних даних, експертні судження та динамічний розвиток атак. Результатом є більш гнучка та адаптивна модель оцінки ризиків, яка підтримує прийняття обґрунтованих рішень для підвищення кібербезпеки, визначення пріоритетів контрзаходів та оптимізації розподілу оборонних ресурсів.

В роботі [33] «система захисту розглядається в комплексі, як декілька захисних механізмів з можливими взаємозв'язками і власною ефективністю протидії на певні види загроз. ... На відміну від відомих моделей модель процесу захисту інформації з повним перекриттям загроз дозволяє враховувати внутрішні взаємозв'язки загроз, системи захисту інформації таоб'єктів захисту, а також дозволяє розкрити структуру системи, виділити та оцінити ефективність роботи бар'єрів, що перекривають області вразливостей механізмів захисту інформації».

У статті [12] розглядається питання інформаційної безпеки в середовищі промислового Інтернету речей (англ. Industrial Internet of Things, IIoT), де

оцінка ризиків інформаційної безпеки ускладнюється неоднорідністю системи, її динамічним характером, розподіленою мережевою інфраструктурою, відсутністю стандартів та інструкцій, а також посиленням наслідків порушень безпеки. Враховуючи ці фактори, оцінка ризиків інформаційної безпеки в IIoT вимагає комплексного підходу, адаптованого до особливостей та вимог конкретної системи та галузі. Необхідно використовувати спеціалізовані методи оцінки ризиків та враховувати контекст та особливості системи. Запропоновано метод оцінки ризиків інформаційної безпеки в IIoT, заснований на математичному апараті теорії нечітких множин. У цій роботі аналізуються загрози інформаційній безпеці для систем IIoT, з яких вибираються найбільш значущі критерії. Правила, на основі яких приймаються рішення, формулюються у вигляді логічних формул, що містять вхідні параметри. Використовуються три системи нечіткого висновку: одна для оцінки ймовірності реалізації загрози, інша для оцінки ймовірної шкоди та кінцева для оцінки ризику інформаційної безпеки для системи IIoT. На основі запропонованого методу наведено приклади розрахунку оцінки ризиків інформаційної безпеки в середовищі IIoT.

Висновки до розділу 2

У другому розділі кваліфікаційної роботи проведено аналіз методів формалізації і моделювання процесу оцінювання критичності активів, що дозволило перевести теоретичні вимоги нормативно-правових актів у площину чітких інженерних рішень.

Основними результатом цього розділу є визначення основ побудови інформаційної моделі, зокрема, доцільно використовувати апарат теорії графів і теорію нечітких множин. Це дозволяє алгоритмічно врахувати каскадний ефект і, на відміну від статичного підходу НД ТЗІ 3.6-005-21, математично описати архітектуру розподіленої установи та врахувати залежності між активами.

РОЗДІЛ 3. РОЗРОБКА ІНФОРМАЦІЙНОЇ МОДЕЛІ ОЦІНЮВАННЯ КРИТИЧНОСТІ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

3.1 Модель взаємозв'язку між впливовими факторами

Для побудови адекватної автоматизованої системи оцінювання критичності необхідно виконати математичну формалізацію структури об'єкта дослідження. Сучасне підприємство або установа є складною системою, де вихід з ладу одного технічного компонента може паралізувати критичні бізнес-процеси. Згідно НД ТЗІ 3.6-005-21 ІС та дані розглядаються ізольовано, що не дозволяє врахувати каскадні ефекти відмови та приховані технологічні залежності.

Для вирішення цієї проблеми пропонується побудувати математичну модель оцінювання критичності інформації та ІС на основі теорії графів та множин, щоб дає змогу відобразити ієрархічну структуру організації та простежити шлях впливу від первинного цифрового активу до кінцевого процесу. Згідно з методологічними принципами стандарту ДСТУ ISO/IEC 27005:2023 [20] та фреймворку NIST SP 800-60 [15], об'єкт оцінювання має бути декомпонований на три взаємопов'язані рівні:

− організаційний рівень (рівень бізнес-процесів): сукупність функцій, критичних послуг та процесів установи (організації, підприємства, порушення яких призводить до прямих збитків, юридичної відповідальності або загрози національній безпеці;

− системний рівень (рівень інформаційних систем): сукупність програмних комплексів, автоматизованих робочих місць, серверів, мережевого обладнання та хмарних сервісів, які забезпечують виконання зазначених процесів;

− рівень даних (інформаційний рівень): безпосередньо масиви даних, бази даних, державні реєстри, файлові сховища, конфіденційність, цілісність чи доступність яких підлягає захисту.

Для математичного опису цієї структури об'єкт оцінювання представляється у вигляді орієнтованого багатодольного (ієрархічного) графа

$$G = (V, E), \tag{3.1}$$

де V - множина вершин, що відображають активи всіх рівнів;

E — множина орієнтованих дуг, що задають напрямок залежностей між ними.

Множина вершин V розподіляється на три неперетинні підмножини:

$$V = P \cup S \cup D, \tag{3.2}$$

де $P = \{p_1, p_2, \ldots, p_n\}$ — множина вершин, що репрезентують критичні бізнес-процеси або функції організації;

$S = \{s_1, s_2, \ldots, s_m\}$ — множина вершин, що відповідають окремим інформаційним системам, сервісам чи апаратним вузлам;

$D = \{d_1, d_2, \ldots, d_k\}$ — множина вершин, які відображають конкретні типи інформації, бази даних чи електронні реєстри;

n — загальна кількість процесів;

m — кількість ІС;

k — кількість інформаційних активів.

Наявність орієнтованого ребра $e_{ij} = (v_i, v_j) \in E$ означає, що функціонування або безпека активу v_i безпосередньо залежить від стану та безпеки активу v_j. Напрямок дуг у даній моделі доцільно орієнтувати від елементів нижчого рівня (дані) до елементів вищого рівня (процеси), що відображає трансляцію критичності знизу вгору.

Таким чином, дуги можуть існувати лише між суміжними або спорідненими шарами:

$$E \subseteq (D \times S) \cup (S \times P) \cup (S \times S). \tag{3.3}$$

Наявність ребер типу (s_i, s_j) відображає внутрішні архітектурні залежності між самими інформаційними системами (наприклад, залежність веб-сервісу від працездатності сервера автентифікації чи DNS-сервера).

Для повної формалізації взаємозв'язків граф G описується матрицею суміжності або сукупністю матриць зв'язку між рівнями. Зокрема, зв'язок між даними та інформаційними системами задається матрицею A_{DS} розмірністю $k \times m$, а зв'язок між ІС та процесами — матрицею A_{SP} розмірністю $m \times n$.

Кожне ребро $e_{ij} \in E$ додатково характеризується ваговим коефіцієнтом $w_{ij} \in [0, 1]$, який відображає ступінь залежності. Якщо $w_{ij}=1$, то порушення безпеки дочірнього активу повністю руйнує безпеку батьківського активу; якщо $w_{ij}=0$, то залежність відсутня.

Графічну схему побудованої моделі взаємозв'язків та трансляції залежностей між бізнес-процесами, інформаційними системами та даними наведено на рис.3.1.

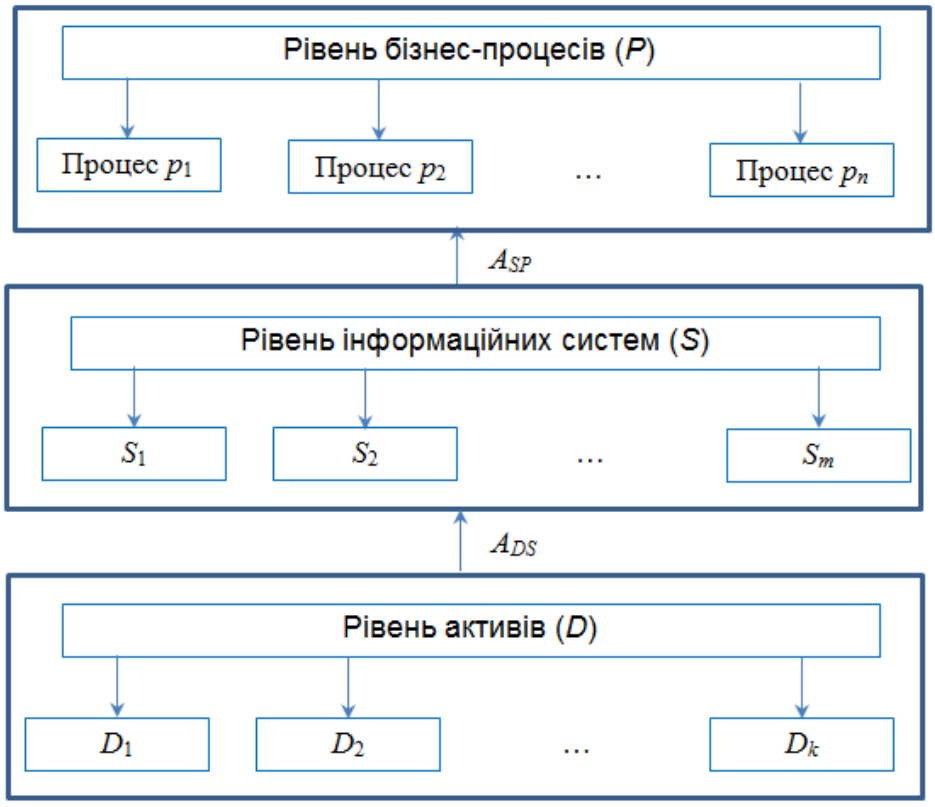

Рисунок 3.1 - Схема взаємозв'язків та трансляції залежностей в моделі

Впровадження такої моделі в алгоритмічну базу кваліфікккааційної роботи роботи дозволяє автоматизувати пошук критичних шляхів та «єдиних точок відмови» (англ. Single Point of Failure) в інфраструктурі організації. Якщо певна база даних d_1 використовується одночасно кількома ІС, які, у свою чергу, забезпечують життєдіяльність усіх ключових процесів установи, то її інтегральний індекс критичності автоматично набуде максимального значення, навіть якщо за первинними ознаками НД ТЗІ 3.6-005-21 вона відносилася до нижчої категорії. Це закладає математичне підґрунтя для наступних етапів розрахунку індексів критичності на основі ризик-орієнтованого підходу.

Переведення розробленої графової моделі у практичну площину автоматизованого розрахунку потребує обґрунтування чіткої системи метрик і критеріїв оцінювання. На відміну від класичного аналізу ризиків, де оцінюється ймовірність реалізації загроз, оцінювання критичності фокусується виключно на наслідках інцидентів безпеки — тобто на масштабі потенційних збитків у разі компрометації активу. Для забезпечення всебічності аналізу оцінювання має здійснюватися диференційовано за кожною з трьох складових класичної тріади безпеки: конфіденційністю (К), цілісністю (Ц) та доступністю (Д). При цьому оцінювання збитків має проводитися з врахуванням як прямих кількісних (фінансових), так і непрямих (репутаційних, юридичних, операційних) втрат.

Для оцінювання збитків пропонується використовувати уніфіковану шкалу, адаптовану під вимоги вітчизняного законодавства та міжнародного фреймворку FIPS 199. Кожен критерій оцінюється за чотирирівневою шкалою:

$$M \in \{0, 1, 2, 3\}, \tag{3.4}$$

де M=0 - вплив відсутній (компрометація активу не несе негативних наслідків);

M=1 - низький рівень впливу (обмежені збитки);

M=2 - середній/помірний рівень впливу (серйозні збитки);

M=3 - високий рівень впливу (катастрофічні збитки).

Для формалізації процедури експертного аналізу визначаємо специфічні критерії збитків для кожної категорії тріади безпеки:

1) метрики оцінювання збитків від порушення конфіденційності ($М_К$):

− юридична відповідальність: оцінюється ступінь порушення Законів України, наприклад Закону «Про захист персональних даних» та інших. Високий рівень (3) присвоюється у разі витоку інформації, що становить державну таємницю або призводить до кримінальної відповідальності керівництва.

− репутаційні збитки: оцінюється рівень втрати довіри з боку громадян, клієнтів або міжнародних партнерів;

2) метрики оцінювання збитків від порушення цілісності ($М_Ц$):

− вартість відновлення даних: прямі фінансові та часові витрати на повторне введення, верифікацію або розгортання інформаційних ресурсів з резервних копій;

− точність прийняття рішень: оцінюється ймовірність того, що викривлення інформації в ІС призведе до хибних управлінських чи технологічних кроків із небезпечними наслідками;

3) метрики оцінювання збитків від порушення доступності ($М_Д$):

− допустимий час простою (англ. Recovery Time Objective, *RTO*): критична метрика часового інтервалу, протягом якого система може залишатися непрацездатною без завдання незворотної шкоди бізнес-процесам;

− масштаб операційних збитків: кількість користувачів, транзакцій або технологічних об'єктів, які одночасно втрачають доступ до сервісу.

Для наочності критерії визначення рівнів збитків зведено у матрицю критеріїв (табл.3.1).

Розроблена система метрик дозволяє сформувати вектор первинних оцінок для будь-якого інформаційного активу установи:

$$V_{вплив} = (К_{вплив}, Ц_{вплив}, Д_{вплив}). \quad (3.5)$$

Таблиця 3.1 - Матриця критеріїв оцінювання збитків за тріадою безпеки

Рівень збитків	Конфіденційність (К)	Цілісність (Ц)	Доступність (Д)
0: Відсутній	Інформація є відкритою, розголошення не завдає шкоди.	Модифікація виявляється автоматично і не впливає на процеси.	Простої системи непомітні для користувачів і процесів.
1: Низький	Витік даних обмеженого доступу, що не містять персональних даних чи таємниці	Потрібне незначне відновлення; робота процесів не порушується.	*RTO* > 24 годин; збитки мають локальний характер.
2: Середній	Компрометація значних масивів персональних даних або ОКІІ	Модифікація викривляє звітність, викликає серйозні збої	1 година≤*RTO* ≤ 24 години; зупинка підрозділів.
3: Високий	Витік службової інформації або держтаємниць,	Повне знищення реєстрів; прийняття хибних рішень	*RTO* < 1 години; каскадна зупинка критичної інфраструктури

На відміну від стандартного підходу NIST SP 800-60, де підсумкова оцінка системи безальтернативно обирається за максимальним значенням компонента, розроблена інформаційна модель передбачає гнучке зважування метрик. Для різних типів ІС пріоритетність властивостей безпеки є різною. Наприклад, для веб-сайту державного органу найкритичнішими є цілісність та доступність, тоді як для бази даних електронного реєстру - конфіденційність і цілісність. З цієї причини в модель впроваджуються вагові коефіцієнти пріоритету властивостей безпеки для конкретного класу систем:

$$\alpha_К + \alpha_Ц + \alpha_Д = 1. \tag{3.6}$$

Для певного активу ІС із заданими коефіцієнтами пріоритету властивостей безпеки $\alpha_К$, $\alpha_Ц$ і $\alpha_Д$ негативні впливи зважуються за формулою:

$$M_{активу} = \alpha_К M_К + \alpha_Ц M_Ц + \alpha_Д M_Д \tag{3.7}$$

Обґрунтована система метрик та диференційованих критеріїв за тріадою безпеки дозволяє позбутися однобічності при оцінюванні активів. Вона забезпечує

інформаційну модель вхідними даними високої точності, що є необхідною умовою для подальшого застосування математичного апарату обробки невизначеності та розрахунку інтегральних індексів критичності систем.

Для забезпечення динамічності узагальненої моделі застосуємо перерахунок індексу критичності з урахуванням топології графа взаємозв'язків активів $G=(V, E)$. Інтегральний індекс критичності ІС у момент часу t $(I_{crit}(s_j, t))$ формується як функція від її власної локальної критичності та максимальної критичності суміжних систем чи бізнес-процесів, які від неї залежать:

$$I_{crit}(s_j, t) = \max\left(L_{crit}(s_j), \max_{v \notin T(s_j)} \left(w(s_j, v) \cdot I_{crit}(v, t) \right) \right), \quad (3.8)$$

де $T(s_j)$ – множина вершин (ІС або бізнес-процесів), для яких s_j є забезпечуючим або дочірнім фактором;

$w(s_j, v)$ – вага ребра, що відображає ступінь залежності між активами.

Завдяки рівнянню (3.8) реалізується «трансляція критичності знизу вгору». Якщо у момент часу t змінюється статус або критичність бізнес-процесу p_1 (наприклад, підприємство впроваджує нову критичну послугу), то інформаційна модель автоматично перераховує та підвищує індекси критичності для всіх пов'язаних систем s_j та баз даних d_i по всьому ланцюгу залежностей.

Для демонстрації динамічних властивостей моделі та процесу зміни категорій систем під впливом операційного контексту складемо приклад матриці станів та переходів рівнів критичності (табл.3.2).

Формування узагальненої інформаційної моделі дозволяє вирішити головні протиріччя існуючих підходів — суб'єктивізм та статичність. Модель не просто присвоює системі жорстку категорію (наприклад, «ОКІІ категорії критичності 3» чи «ІС категорії критичності 2»), а розраховує гнучкий індекс, який безпосередньо інтегрується в загальну систему менеджменту ризиків організації.

Таблиця 2.3 - Матриця динамічних переходів рівнів критичності ІС залежно від контексту

Початковий індекс $I_{crit}(t_0)$	Зміна операційного контексту (Подія)	Зміни в моделі	Новий індекс $I_{crit}(t_1)$
Низький (0.0 - 0.3)	Систему підключено до контуру критичного бізнес-процесу p_k	Поява ребра (s_j, p_k) з вагою w_{jk}=1.0 у матриці суміжності графа A_{SP}	Високий (0.7 - 1.0)
Середній (0.4 - 0.6)	Дані системи дубльовано в ізольовану хмару (налаштовано бекап)	Зниження локальної метрики збитків від втрати доступності $M_Д$	Низький (0.0 - 0.3)
Середній (0.4 - 0.6)	З'явилася критична вразливість типу 0-day для ОС сервера системи (дані CERT-UA)	Збільшення вагового коефіцієнта вразливості та ризику каскадного впливу	Високий (0.7 - 1.0)

Ваги ребер і збитки можуть задаватися нечіткими, тоді слід вводити відповідні лінгвістичні змінні, визначати фкнуції належності їх нечітких множин і формувати систему нечітких правил для визначення інтегральної критичності, наприклад:

$$«ЯКЩО\ (M_К\ є\ Високими)\ ТА\ (M_Ц\ є\ Середніми)\ ТА\ (M_Д\ є\ Низькими),$$
$$ТО\ (I_{crit}\ є\ Високою)». \quad (3.9)$$

Результати розрахунку узагальненої моделі є основою для автоматичного вибору необхідного комплексу технічних та організаційних заходів захисту інформації в автоматизованій системі, оптимізуючи витрати на кібербезпеку в умовах обмежених ресурсів

3.2 Розробка базових алгоритмів

Проведені у Розділі 1 аналіз нормативно-правової і аналіз у Розділі 2 матеріалів методичного характеру дозволяють побудовані наступні базові

алгоритми для розроблюваної інформаційної моделі оцінювання критичності інформації та ІС.

По-перше, це узагальнений алгоритм категоризації об’єктів критичної інформаційної інфраструктури (рис.3.1).

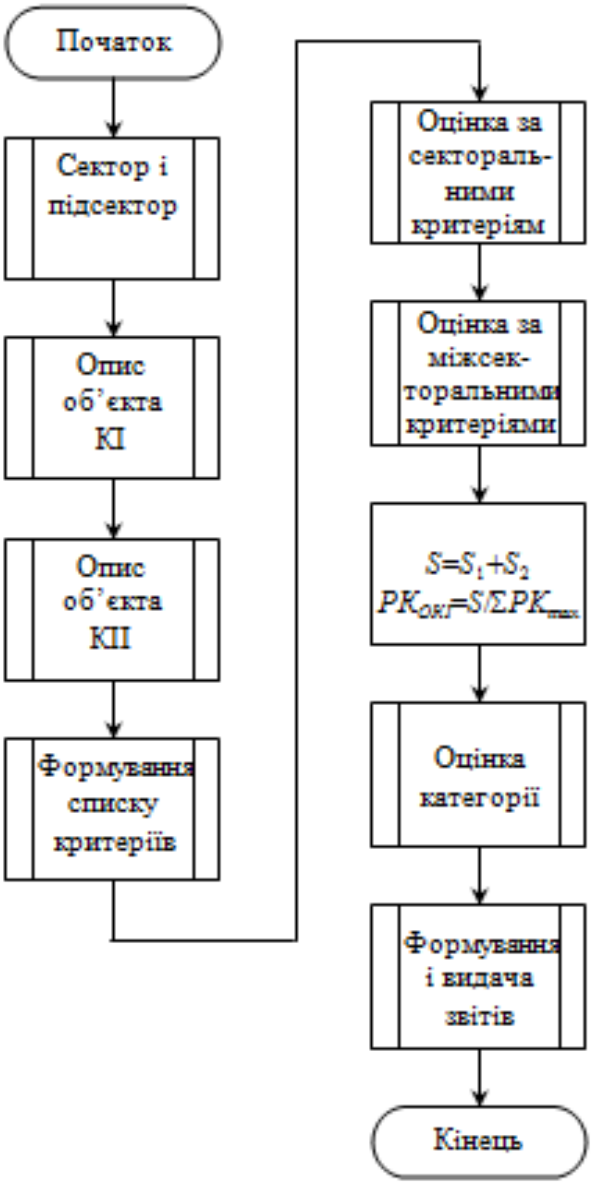

Рисунок 3.2 – Узагальнений алгоритм оцінювання критичності ОКІІ

Згідно з алгоритмом рис.3.2. спочатку отримуються бальні експертні оцінки ступенів критичності наслідків порушення функціонування ОУІ за секторальними і міжсекторальними критеріями, а потім розраховується нормована оцінка рівня

критичності об’єкта, за значенням якої його відносять до певної категорії критичності за алгоритмом рис.3.3. Цих категорій 4. І найбільш критичною є перша категорія.

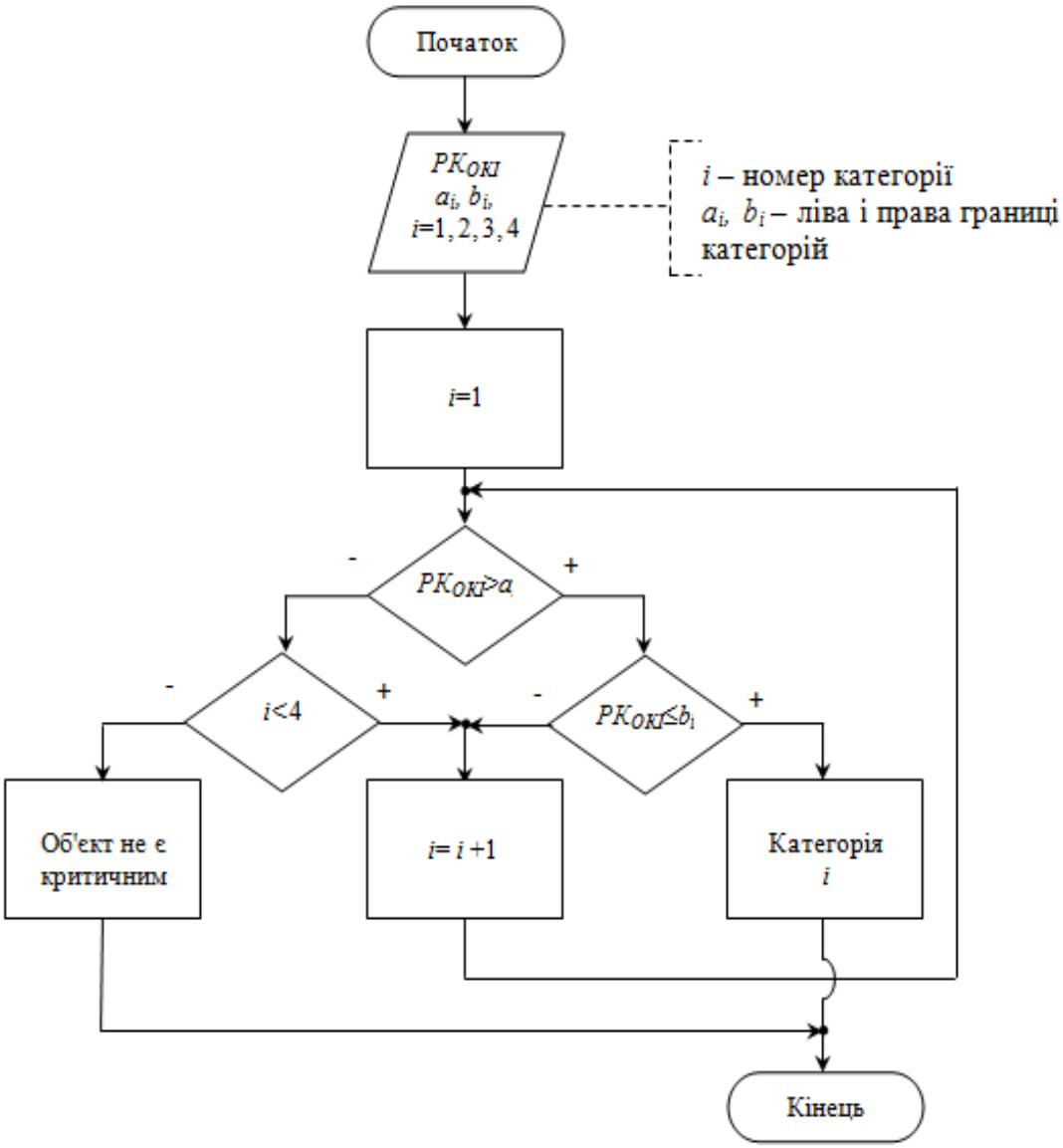

Рисунок 3.3 – Алгоритм категорування критичності ОКІІ

Згідно НД ТЗІ 3.6-005-21 рівні критичності отримують якісні оцінки (В, С, Н) і визначаються, виходячи з тяжкості наслідків порушення конфіденційності, цілісності та доступності інформації, за розробленими і представленими на рис.3.4-3.6 алгоритмами.

На рис.3.4-3.6: PK_{jm}, $PKrj$, $PK_{IC} \in$ {Низький, Середній, Високий}.

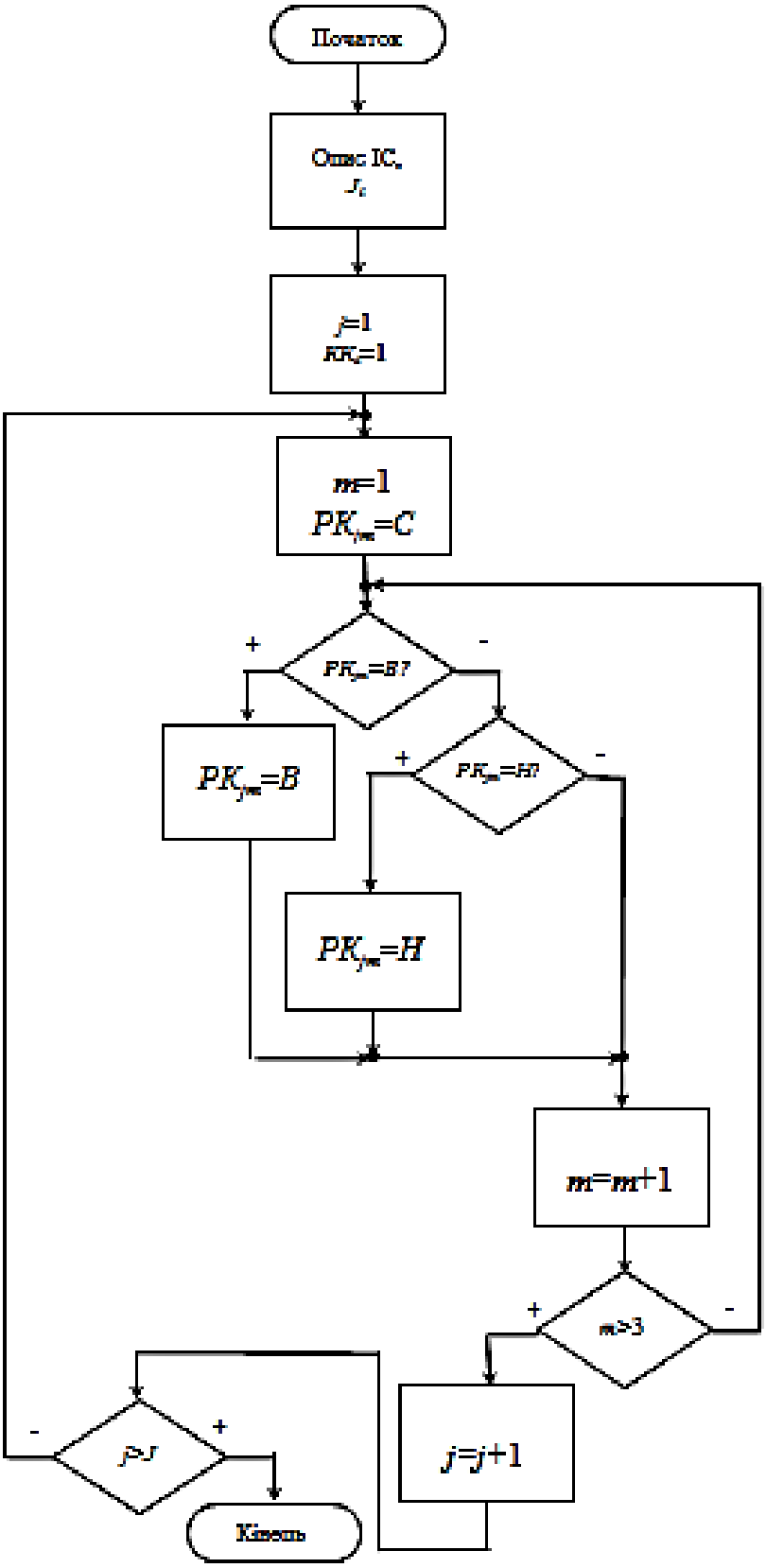

Рисунок 3.4 – Алгоритм оцінювання критичності інформації в активах

m=1 – конфіденційність; m=2 – цілісність; m=3 – доступність;

J – загальна кількість активів.

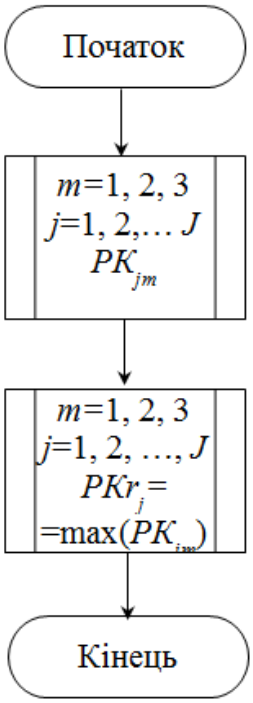

Рисунок 3.5 – Алгоритм оцінювання критичності активів ІС

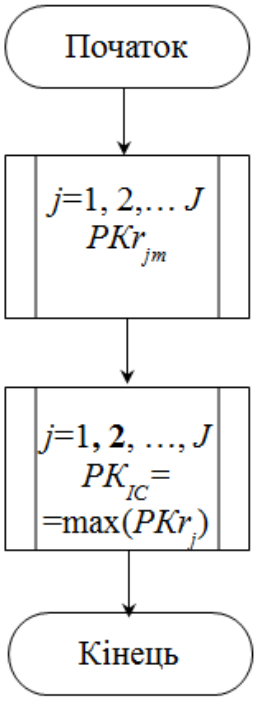

Рисунок 3.6 – Алгоритм оцінювання критичності ІС

Уніфіковані вимоги Міжнародної асоціації класифікаційних товариств IACS E22 [9] визначають 3 категорії критичності, з яких найбільш критичною є третя

категорія. При цьому розглядаються загрози, які не виникнуть, можуть виникнути або негайно виникнуть для безпеки людини (i=1), екології (i=2) і живучості судна (i=2). На рис.3.7 наведено алгоритм оцінювання критичності суднових комп'ютеризованих систем з перевіркою умови $У_i$=«Вплив наявний?».

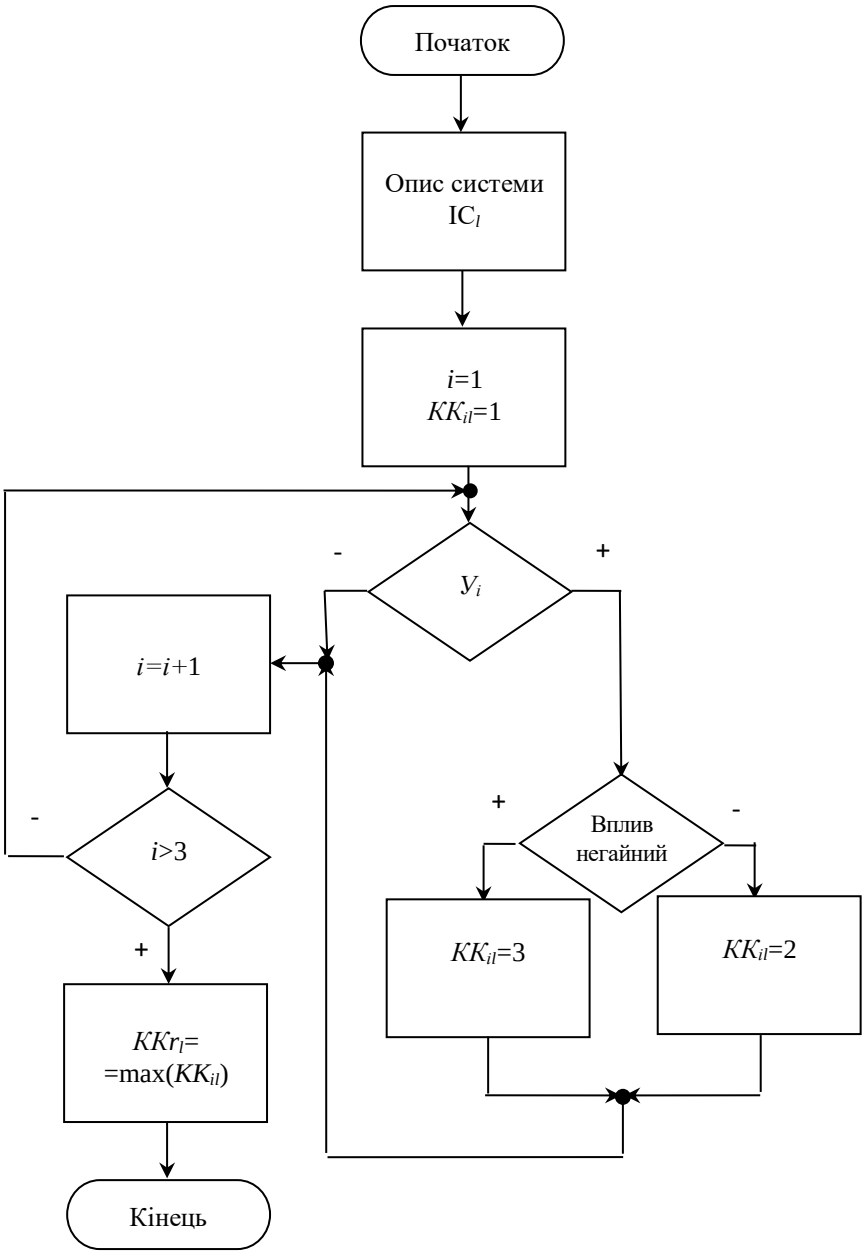

Рисунок 3.7 – Алгоритм оцінювання категорії критичності ІС за IACS E22

В IACS E22 При цьому побічно згадується, що комп'ютеризовані системи можуть впливати одна на одну. Для врахування цього взаємного валиву було розроблено алгоритм, наведений на рис.3.8.

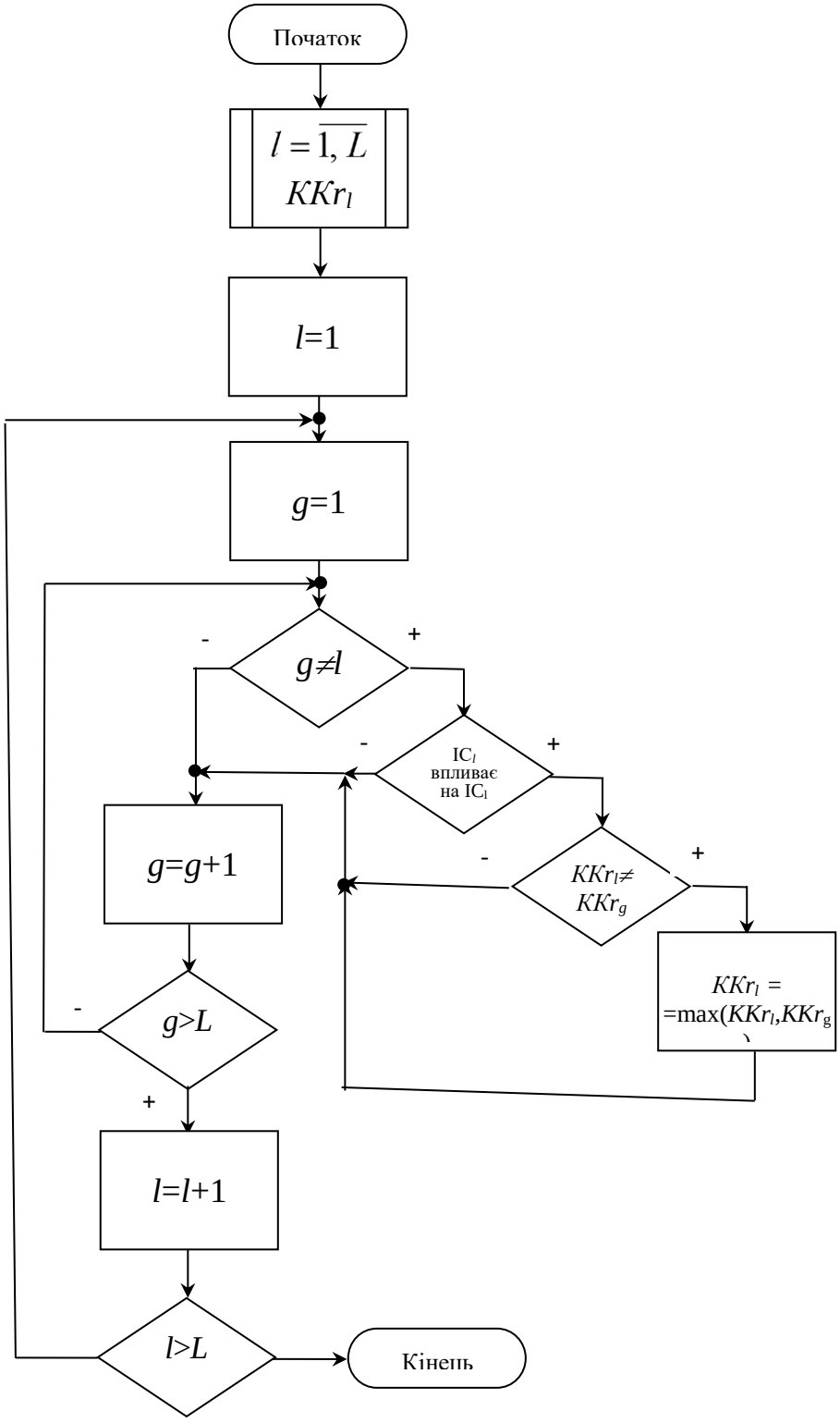

Рисунок 3.8 – Алгоритм перевизначення категорій критичності ІС з врахуванням взаємного впливу ІС за IACS UR E22

Слід зауважити, що алгоритм визначення взаємного впливу ІС (рис.3.8) потрібно пройти не один раз, а повторювати доти, поки категорії критичності

не перестануть змінюватися, тобто необхідним є додатковй механізм контролю збіжності даного алгоритму.

3.3 Розробка структури інформаційної моделі оцінювання критичності інформації та інформаційних систем

Розроблена стрктура інформаційної моделі наведена на рис.3.8 і містить:

1) інтерфейс адміністратора, який може вносити зміни у всі інші блоки;

2) інтерфейс користувача, який дозволяє

− вводити дані в блок «Дані користувача», обов'язково використовуючи при цьому вибір з блоку «Вбудовані дані» для даних, які зазначені у нормативно-правових актах, наприклад назву сектору і підсектору для ОКІ. Інші дані, які є описами вводяться користувачем під його відповідальність і використовуються при формування звітів за обраним користувачем типовим форматом;

− формулювати вимоги щодо оцінювання критичності інформації та інформаційних систем у вигляді запитів до «Блоку оцінювання»;

− обирати типовий формат звіту у вигляді запиту до «Блоку формування звітності»;

− отримувати звіт з оцінювання критичності інформації та інформаційних систем у заданому форматі;

3) «Блок даних», який містить блоки «Вбудовані дані» і «Дані користуівча». До вбудованих даних, зокрема, відносяться типові форми звітів, які доступні користувачу для вибору;

4) «Блок оцінювання», в якому на вимогу користувача може здійснюватися оцінювання рівнів і категорій критичності інформації, активів, ІС, ОКІ та ОКІІ , в тому числі - визначатися інтегральний індекс критичності;

5) «Блок формування звітності» у форматі, обраному користувачем за результатами, отриманими в «Блоці оцінювання».

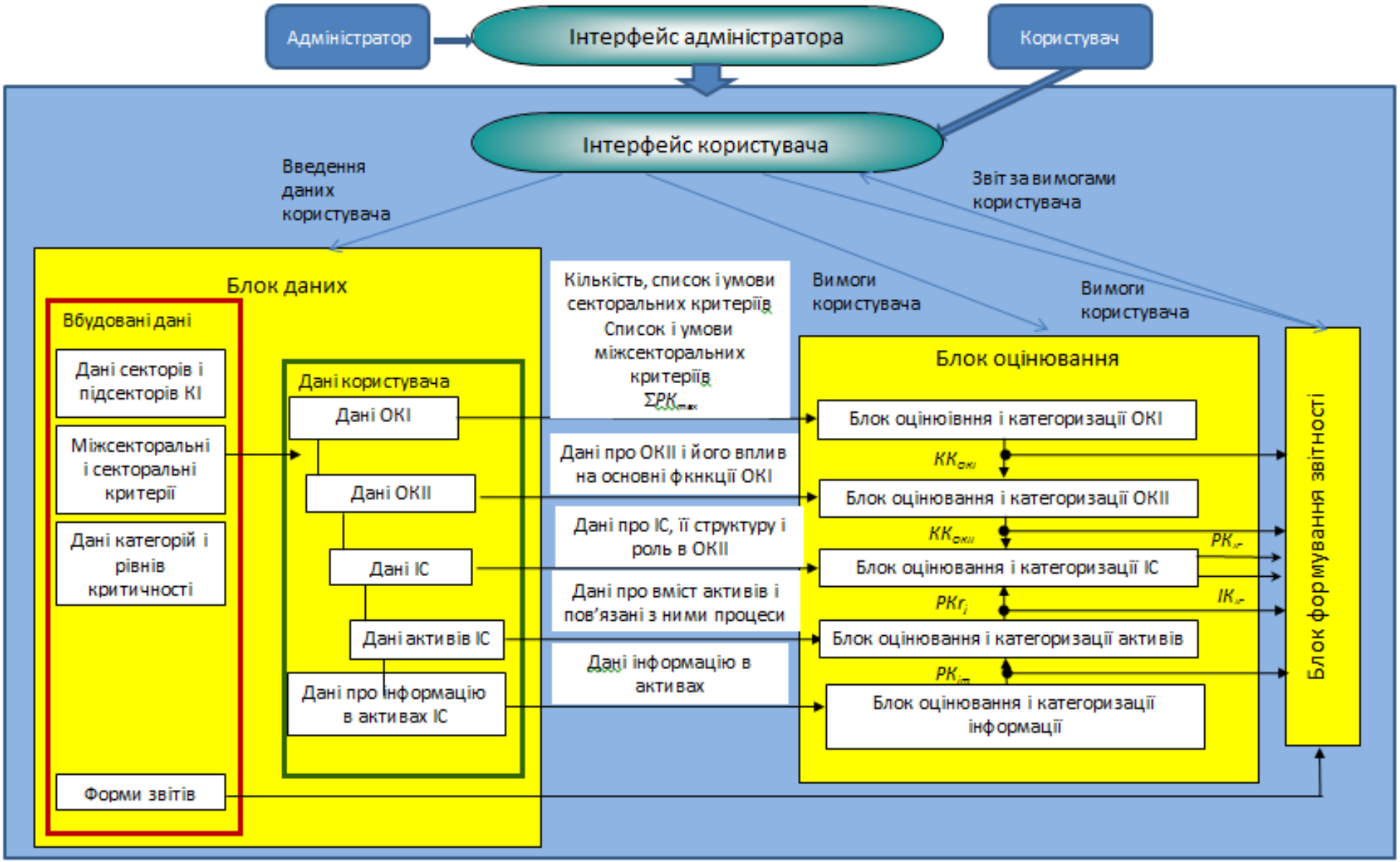

Рисунок 3.9 – Структура інформаційної моделі

Висновки до розділу 3

У даному розділі розроблено інформаційну модель оцінювання критичності, яка формалізує залежності між впливовими факторами, і базові алгоритми для автоматизованого визначення за даними користувача рівнів і категорій критичності інформації, активів, ІС, ОКІ, ОКІІ, інтегрального індексу критичності.

Головною особливістю побудованої моделі є алгоритмічне врахування каскадного ефекту, завдяки якому зміна операційного контексту або критичності бізнес-процесу автоматично транслюється знизу вгору по графу залежностей, миттєво перераховуючи індекси для всіх забезпечуючих систем та активів в режимі реального часу.

РОЗДІЛ 4. АПРОБАЦІЯ БАЗОВИХ АЛГОРИТМІВ ІНФОРМАЦІЙНОЇ МОДЕЛІ ОЦІНЮВАННЯ КРИТИЧНОСТІ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

4.1 Опис бази даних

Для апробації основних процедур інформаційної моделі було створено базу даних MS Access, титульна форма якої наведена на рис.4.1.

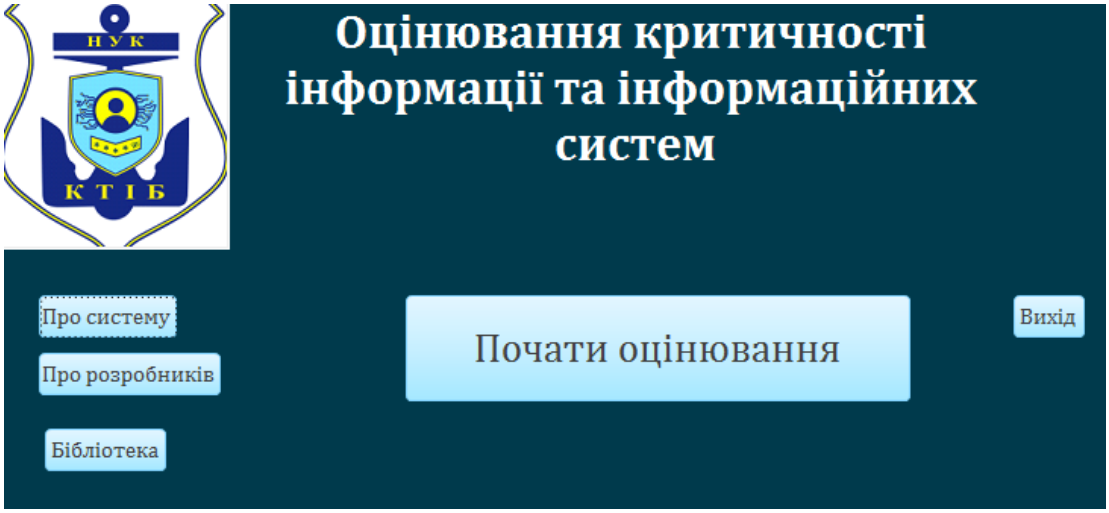

Рисунок 4.1 – Титульна форма розробленої бази даних

Список таблиць розробленої бази даних наведений на рис.4.2.

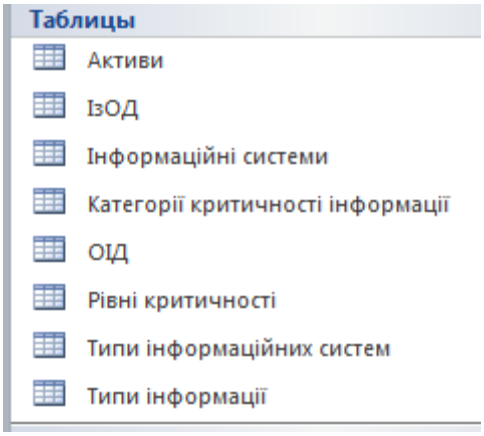

Рисунок 4.2 – Об’єкти «Таблиця» розробленої бази даних

4.2 Введення даних

На рис.4.3-4.7 наведено приклади заповнення створених таблиць.

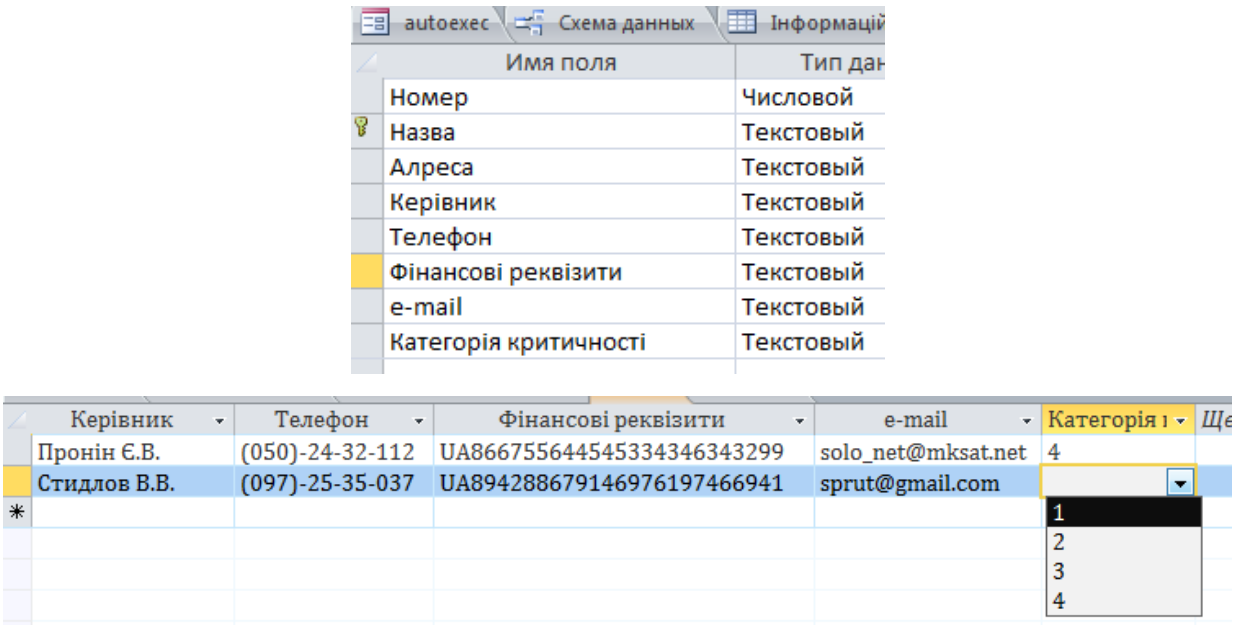

Рисунок 4.3 – Таблиця «ОІД»: структура і заповнення з використанням підстановки

В таблиці «ОІД» категорія критичності задається з вбудованої таблиці підстановки згідно з актом категоризації, який передбачається наявним.

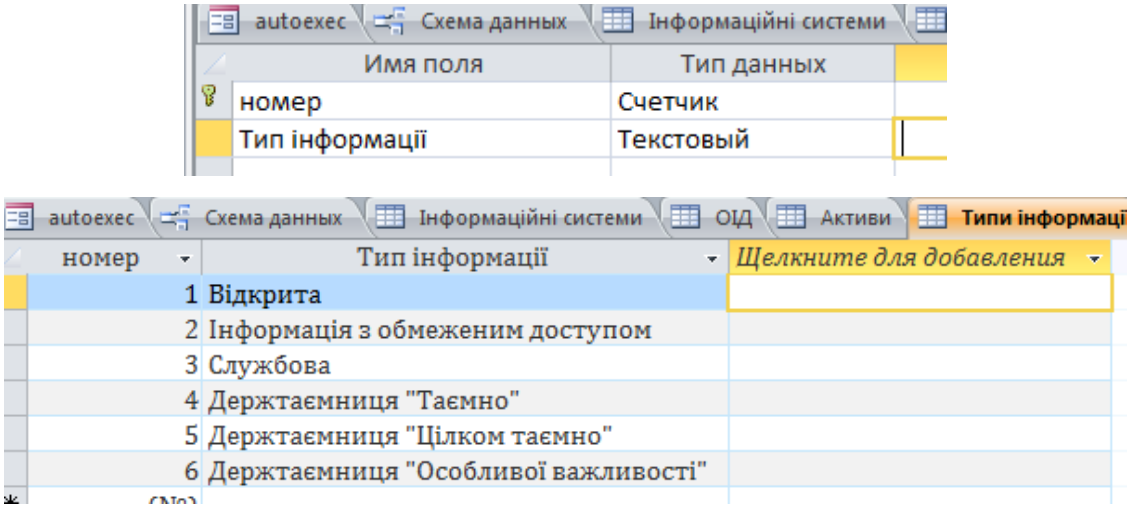

Рисунок 4.4 – Таблиця «Типи інформації»: структура і заповнення

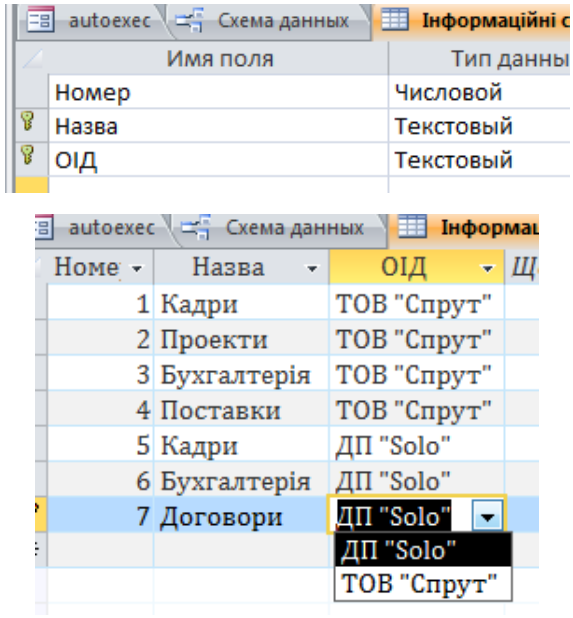

Рисунок 4.5 – Таблиця «Інформаційні системи»: структура і заповнення з використанням підстановки

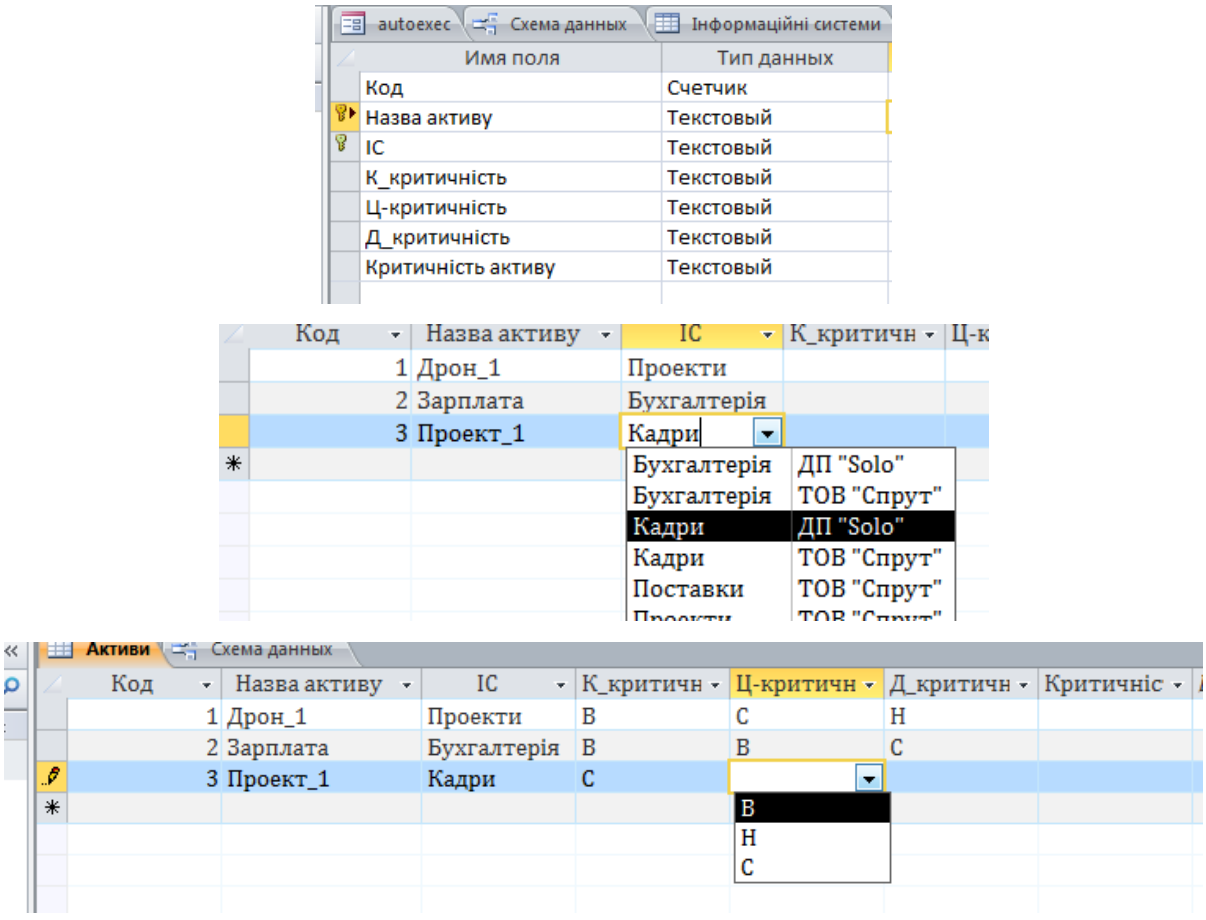

Рисунок 4.6 – Таблиця «Активи»: структура і заповнення з використанням підстановки

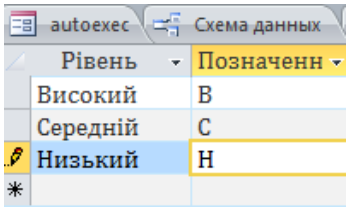

Рисунок 4.7 – Таблиця підстановки «Рівні критичності»

4.3 Визначення критичності інформації та інформаційних систем

Категорія критичності ОКІ задається в таблиці ОКІ (рис.4.3).

Критичність інформації визначається в таблиці (рис.4.6) або формі «Активи» з використанням вбудованих таблиць підстановки.

Приклад визначення рівня критичності активів у формі «Активи» наведено на рис.4.8 (використовувався Побудувач виразів) і рис.4.9.

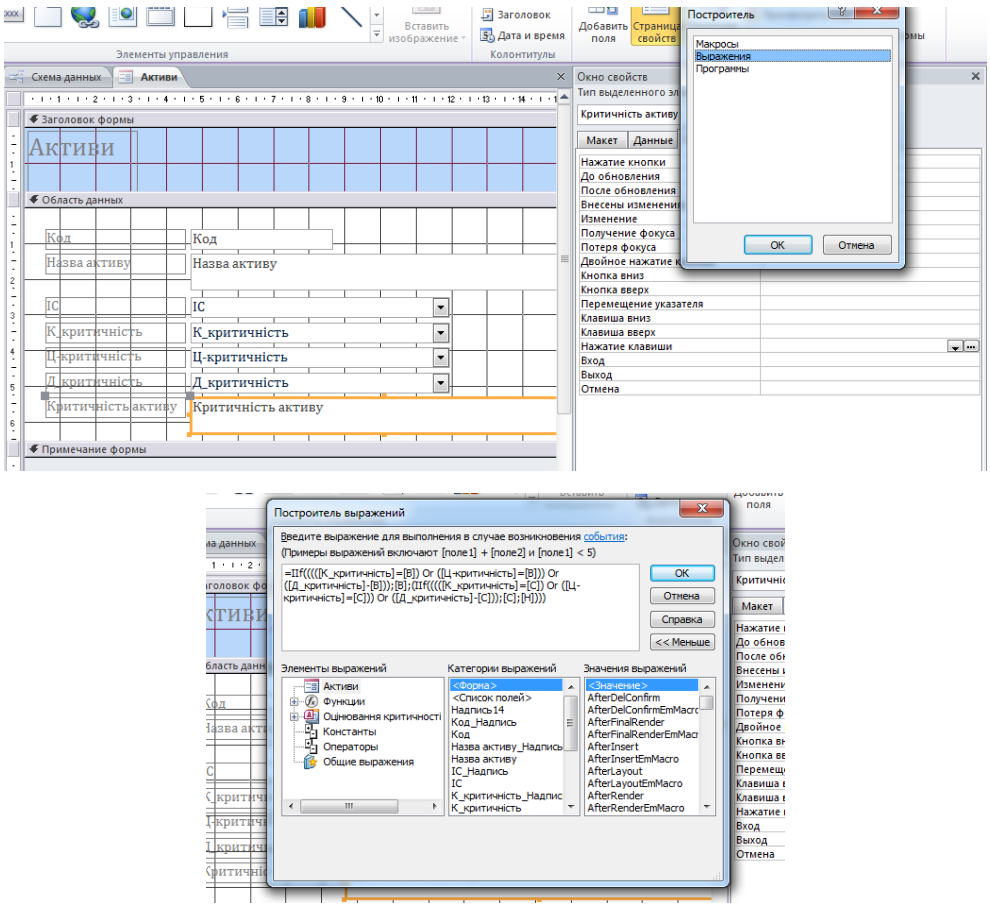

Рисунок 4.8 – Форма «Активи»: створення виразу для визначення критичності активу

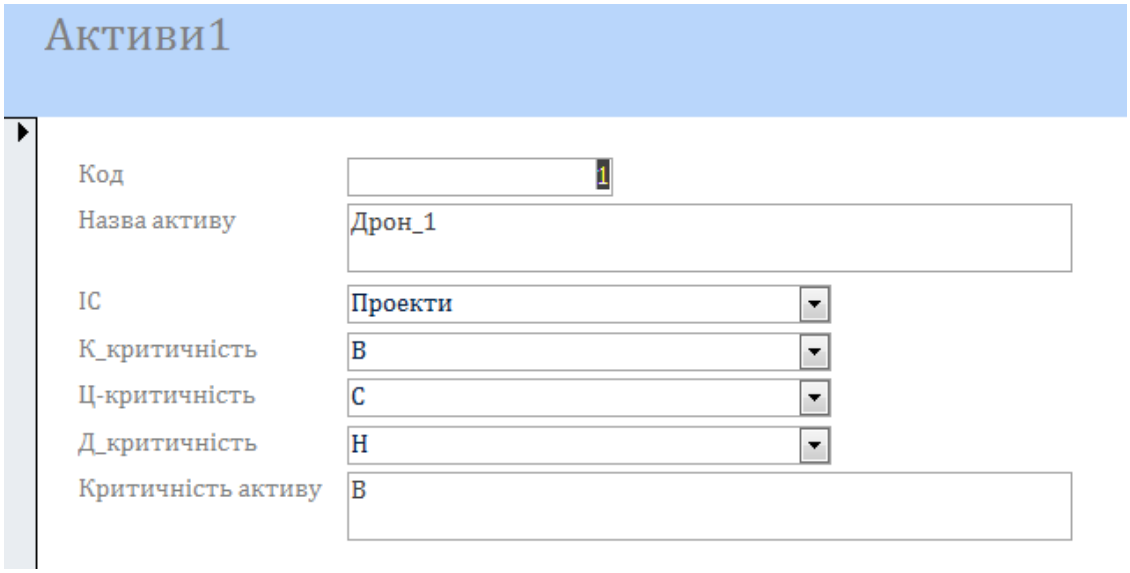

Рисунок 4.9 – Форма «Активи»: результати визначення критичності активу

З взаємопов'язаних таблиць «Активи» та «Інформаційні системи» після визначення рівня критичності активів можна отримати вибірку активів для заданої ІС з визначеними рівнями критичності (рис.4.10). За результатами запиту аналогічно рис.4.9 шукається рівень критичності ІС у звіті.

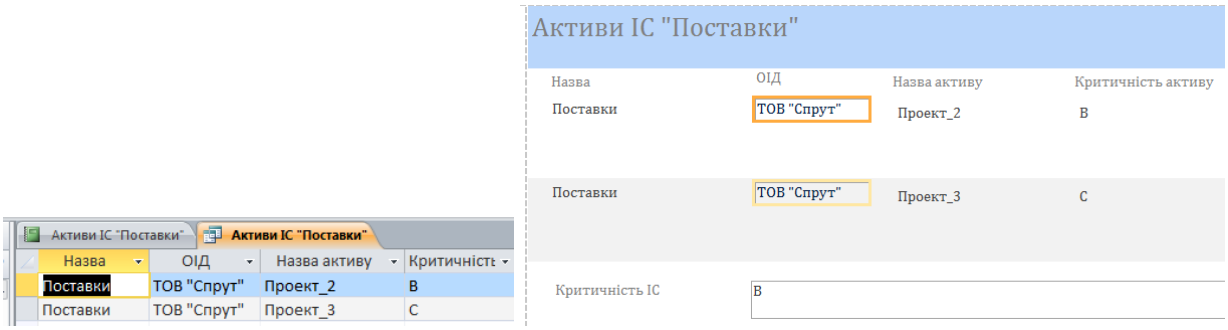

Рисунок 4.10 – Результати запиту на вибірку і категорування ІС

Висновки до розділу 4

Проведена апробація підтвердила працездатність розроблених в Розділі 3 даної кваліфікаційної роботи алгоритмів та адекватність розробленої інформаційнох моделі оцінювання критичності інформації та інформаційних систем.

ВИСНОВКИ

У даній кваліфікаційній роботі:

− проведено аналіз чинних міжнародних та національних стандартів у сфері категоріювання активів та виявлені недоліки існуючих підходів до оцінки критичності інформаційних систем;

− розроблено інформаційну модель оцінювання критичності, яка формалізує залежності між впливовими факторами, і базові алгоритми для автоматизованого розрахунку інтегрального індексу критичності;

− проведено апробацію розроблених алгоритмів і підтверджено адекватність та працездатність моделі.

Розроблені алгоритми та інформаційна модель мають практичну значимість. Результати роботи можуть бути використані під час проєктування СБІ та в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ARMIC. (n.d.). https://www.armis.com/

2. AXONIUS PLATFORM : Axonius Platform Overview. (n.d.). https://docs.axonius.com/docs/using-axonius-overview

3. Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. *Carnegie Mellon University. Octave Allegro: User Guide, Version 1.0. Pittsburgh: Software Engineering Institute*, 2007. 82 p. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). (2022). *Official Journal of the European Union*. 2022. L 333/80. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

5. EAR. Tools: Environment for the Analysis of Risk. (n.d.). https://www.ar-tools.com/en/tools/index.html

6. ENISA. Interoperable EU Risk Management Framework. (2023). https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

7. ENISA Threat Landscape 2025. (2025). https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

8. FIPS Publication 199. *Standards for Security Categorization of Federal Information and Information Systems*. (2004). https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

9. IACS E22. *Computer-based systems*. (2025). https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e22-rev2-cln-2

10. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. (2022). https://www.iso.org/standard/27001

11. ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*. (2022) https://www.iso.org/standard/80585.html

12. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., Salykbayeva, A. (2023). Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry*, Volume 15, Issue 10. https://www.mdpi.com/2073-8994/15/10/1958

13. Nakonechna, Yu., Savchuk, B., Kovalova, A. (2024). Fuzzy logic in risk assessment of multi-stage cyber attacks on operational network structures. *Theoretical and Applied Cybersecurity*. Vol.6 No.2. P.52-65. https://doi.org/10.20535/tacs.2664-29132024.2.318023

14. NIST Special Publication 800-30. Revision 1. *Guide for Conducting Risk Assessments*. (2012). https://csrc.nist.gov/pubs/sp/800/30/r1/final

15. NIST Special Publication 800-60. Volume I. Revision 2. *Guide for Mapping Types of Information and Systems to Security Categories*. (2024). https://csrc.nist.gov/pubs/sp/800/60/r2/iwd

16. What is GRC (Governance, Risk and Compliance)? (n.d.). https://www.ibm.com /think/topics/grc

17. Деякі питання об'єктів критичної інформаційної інфраструктури : *Постанова Кабінету міністрів України* від 9.10.2020 №943. (Редакція - 01.01.2026). https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

18. Деякі питання об'єктів критичної інфраструктури : *Постанова Кабінету міністрів України* від 9.10.2020 №1109. (Редакція - 22.05.2026). https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text

19. ДСТУ ISO/IEC 27001:2023. *Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги***.** (ISO/IEC 27001:2022, IDT). (2023). https://online.budstandart.com/ua/catalog/searchdoc.html?request=%D0%94%D0%A1%D0%A2%D0%A3+ISO%2FIEC+27001%3A2023+%28ISO%2FIEC+27001%3A2022%2C+IDT%29&langbs=ua

20. ДСТУ ISO/IEC 27005:2023. *Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки.* (ISO/IEC 27005:2022, IDT) (2023). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400

21. Задерейко, О., Трофименко, О., Єленич, С., Логінова, Н., & Гура, В. (2025). Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 4(28), 57–70. https://doi.org/10.28925/2663-4023.2025.28.735

22. Злочевська, О. В. (2024). Система підтримки прийняття рішень щодо категоризації об'єктів критичної інфраструктури. *Матеріали XII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». Миколаїв: НУК, 2024*. С.85-91. https://nuos.edu.ua/wp-content/uploads/2025/06/SPIBT-2024.pdf

23. Зниження кількості кіберінцидентів, складніша соціальна інженерія та уніфікація зброї хакерів: звіт CERT-UA за II півріччя 2025 року. (n.d.). https://cip.gov.ua/ua/news/znizhennya-kilkosti-kiberincidentiv-skladnisha-socialna-inzheneriya-ta-unifikaciya-zbroyi-khakeriv-zvit-cert-ua-za-ii-pivrichchya-2025-roku

24. Іванченко, Є. В., Корченко, О. Г. (2024). Оцінювання стану кіберзахисту об’єктів критичної інформаційної інфраструктури. *Матеріали X Міжнародної науково-практичної конференції. Актуальні питання забезпечення кібербезпеки та захисту інформації. Київ. 2024*. С.61-63. https://www.researchgate.net/publication/384064239_VIKORISTANNA_ALGORITMIV_MASINNOGO_NAVCANNA_V_AVTOMATIZACII_UPRAVLINNA_BIZNES-PROCESAMI_DLA_ZMENSENNA_RIZIKIV_KIBERBEZPEK

25. Кібер-загрози: Україна. Аналітика за II півріччя 2025 року. (n.d.). https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=74645&embedded=true&a=bi

26. Кіберзахист критичної інфраструктури переходить на ризик-орієнтовану модель: Уряд оновив вимоги. https://cip.gov.ua/ua/news/kiberzakhist-kritichnoyi-infrastrukturi-perekhodit-na-rizik-oriyentovanu-model-uryad-onoviv-vimogi

27. Коротенко, С. А. (2024). Використання алгоритмів машинного навчання в автоматизації управління бізнес-процесами для зменшення ризиків кібербезпеки. *Матеріали X Міжнародної науково-практичної конференції. Актуальні питання забезпечення кібербезпеки та захисту інформації. Київ. 2024.* С.61-63. https://www.researchgate.net/publication/384064239_VIKORISTANNA_ALGORITMIV_MASINNOGO_NAVCANNA_V_AVTOMATIZACII_UPRAVLINNA_BIZNES-PROCESAMI_DLA_ZMENSENNA_RIZIKIV_KIBERBEZPEK

28. Костюк, Ю. В., Складанний, П.М., Гулак, Г.М., Бебешко, Б.Т., Хорольська, К.В., Рзаєва. С.Л. (2025). *Системи захисту інформації : підручник*. Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 887 с. https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf

29. НД ТЗІ 3.6-004-21. (2021). *Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці*. https://cip.gov.ua/services/cm/api/attachment/download?id=53375

30. НД ТЗІ 3.6-005-21. (2021). *Порядок категоріювання безпеки інформаційної системи та інформації*. https://cip.gov.ua/services/cm/api/attachment/download?id=65412

31. Огляд національної системи кібербезпеки 2025. Аналітичне дослідження. https://www.rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf

32. Палко, Д.В., Мирутенко, Л.В. (2024). Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах. *Кібербезпека: освіта, наука, техніка*. №2(26). 2024. С.487-500. DOI 10.28925/2663-4023.2024.26.731. https://csecurity.kubg.edu.ua/index.php/journal/article/download /731/597/2424

33. Пепа, Ю. В., Хорошко, В. О., Хохлачова, Ю. Є., Аль-Далваш, А. (2024). Методика аналізу та оцінки захищеності систем захисту інформації з урахуванням ступеня перекриття загроз. *Сучасний захист інформації*. №1. 2024. С.69-77. https://doi.org/10.31673/2409-7292.2024.010008

34. Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 : *Постанова Кабінету міністрів України* від 13.11.2025 № 1470. https://zakon.rada.gov.ua/laws/show/1470-2025-%D0%BF#Text

35. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури : *Постанова Кабінету міністрів України* від 19.06.2019 №518. (Редакція - 20.11.2025). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

36. Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту : *Наказ Адміністрації Держспецзв'язку* від 30.01.2026 № 75. https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2026-75-pro-zatverdzhennya-katalogu-zakhodiv-z-kiberzakhistu-bazovikh-zakhodiv-z-kiberzakhistu-formi-planu-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-zakhodiv-z-kiberzakhistu

37. Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури : *Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України* від 14.01.2025 №17. (2025). https://zakon.rada.gov.ua/laws/show/z0375-25#Text

38. Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ : *Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України* від 15.01.2021 №23. (2021). https://zakon.rada.gov.ua/ rada/show/v0023519-21#Text

39. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : *Розпорядження Кабінету міністрів України* від 7.03.2025 №204-р. https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text

40. Про затвердження Положення про організаційно-технічну модель кіберзахисту: *Постанова Кабінету міністрів України* від 29 грудня 2021 р.

№1426. (Редакція від 26.12.2024). https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

41. Про інформацію : Закон України від 12.10.1992 № 2657-XII. *Відомості Верховної Ради України*. 1992. №48, Ст.650. (Редакція від 20.01.2026). https://zakon.rada.gov.ua/laws/show/2657-12#Text

42. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України*. 2022. № 9. Ст. 36. (Редакція від 21.09.2024). https://zakon.rada.gov.ua/laws/show/1882-20

43. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. №45. Ст.403. (Редакція від 19.10.2025). https://zakon.rada.gov.ua/laws/show/2163-19

44. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": *Указ Президента України* від 26.08.2021 №447/2021. https://zakon.rada.gov.ua/laws/show/447/2021#Text

45. Ромака, В. А., Крайовський, В. Я., Гаранюк, П. І., Горпенюк, А. Я. *Технології розслідування інцидентів інформаційної безпеки*. Електронний підручник. (2023). Львів: Вид-во Львівської політехніки, 2023. 340 с. https://vlp.com.ua/files/230739_peredmova.pdf

46. Скіцько, О., Ширшов, Р. (2023). Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об’єктів критичної інфраструктури. *International Science Journal of Engineering & Agriculture*. Vol.2. No.6. 2023. PP.12-22. DOI: 10.46299/j.isjea.20230206.02

47. Турти, М.В. (2024). Зважене оцінювання критичності об’єктів морського та річкового транспорту. *Матеріали XII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». Миколаїв: НУК, 2024.* С.22-28. https://nuos.edu.ua/wp-content/uploads/2025/06/SPIBT-2024.pdf

48. Турти М.В., Злочевська О.В. (2022). Інформаційна модель категоризації об’єктів критичної інфраструктури. Сучасні проблеми

інформаційної безпеки на транспорті: *Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2022*. С.140-147. *https://www.nuos.edu.ua/wp-content/uploads/2023/05/SPIBT-2022-Materiali-s-obkladinkoju.pdf*

49. Шульга, О. А. (2025). Методичні підходи до аналізу бізнес-процесів підприємства. Економіка та суспільство. DOI: 10.32782/2524-0072/2025-79-148. https://www.researchgate.net/publication/397962933_METODICNI_PIDHODI_DO_ANALIZU_BIZNES-PROCESIV_PIDPRIEMSTVA